EXHIBIT S

PGR
PROCURADURIA GENERAL
DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

ANEXO TÉCNICO

ADQUISICIÓN DE SISTEMA PARA LA REALIZACIÓN DE ACTIVIDADES SUSTANTIVAS DE LA PROCURADURÍA GENERAL DE LA REPÚBLICA DENOMINADO "PEGASUS"

DESCRIPCIÓN DE "EL BIEN".

La descripción de **"EL BIEN"** se encuentra precisada en la cotización expedida por **"EL PROVEEDOR"** en fecha 24 de octubre de 2014, misma que se agrega para formar parte del presente acuerdo de voluntades.

Arquitectura de Alto Nivel

El sistema "Pegasus" está diseñado en capas. Cada capa tiene la responsabilidad de formar juntos una solución de análisis y recolección de inteligencia cibernética integral.

Las capas principales y bloques de construcción de los sistemas son:

- **Instalaciones:** Capa de la instalación está a cargo de la emisión de las nuevas instalaciones de agente, actualizar y desinstalar agentes existentes.
- **Recolección de datos:** Capa de la recopilación de datos está a cargo de recoger los datos desde el dispositivo instalado. "Pegasus" ofrece inteligencia integral y completa mediante el empleo de métodos de recolección de cuatro
- **Extracción de datos:** Extracción de los datos todo que existe en el dispositivo sobre la instalación del agente
- **Vigilancia pasiva:** Nuevos datos de llegada al dispositivo
- **Colección Monitor Activo:** Activar la cámara, micrófono, GPS y otros elementos para recopilar datos en tiempo real
- **Colección basada en eventos:** Definir escenarios que activa automáticamente datos específicos colección
- **Transmisión de datos:** La capa de transmisión de datos es la encargada de transmitir los datos a los servidores de comando y control, utilizando la forma más eficiente y segura.
- **Análisis de la presentación:** El componente de presentación análisis es una interfaz de usuario que se encarga de presentar los datos recogidos a los operadores y analistas, convirtiendo los datos de inteligencia. Esto se hace mediante los siguientes módulos:

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

- **Monitoreo en tiempo real:** Presenta los datos recogidos en tiempo real de específico o varios objetivos. Este módulo es muy importante cuando se trata de objetivos sensibles o durante las actividades operacionales, donde cada pieza de información que llega es crucial para la toma de decisiones.
- **Análisis offline:** Avanzado mecanismo de consultas que permite a los analistas consultar y recuperar cualquier pieza de información que se recopila. El mecanismo avanzado proporciona herramientas para encontrar información y conexiones ocultas.
- **Análisis basado en geolocalización:** presenta los datos recogidos en un mapa y conducta consultas basadas en geo.
- **Administración:** es el componente de administración encargado de gestionar el permiso de todo el sistema, seguridad y salud: contactos de extractos mensajes, correos electrónicos, fotos, archivos, ubicaciones, contraseñas, lista de procesos y más
- **Permiso:** el mecanismo de permisos permite al administrador del sistema gestionar los distintos usuarios del sistema. Proporcionar cada uno de ellos el nivel correcto acceso sólo a los datos que se les permite. Esto permite para definir los grupos de la organización que manejan sólo uno o más temas y otros grupos que maneja diferentes temas.
- **Seguridad:** El módulo de seguridad monitorea el nivel de seguridad del sistema, asegurándose de que los datos recogidos se insertan a la base de datos de sistema limpio y seguro para su futura revisión.
- **Salud:** El componente de salud de la solución de "Pegasus" monitorear el estado de todos los componentes asegurándose de que todo está funcionando sin problemas. Monitorea la comunicación entre las diferentes partes, el rendimiento del sistema, la disponibilidad de almacenamiento de información y alertas si algo falla.

Solución de Hardware

Las especificaciones de hardware para el funcionamiento del sistema Pegasus depende del número de agentes instalados concurrentes, el número de estaciones de trabajo, la cantidad de datos almacenados y por cuánto tiempo deben guardarse.

Todo el hardware necesario es suministrado con el sistema al despliegue y requerir personalización local que tiene que ser manejado por el cliente en función de que las direcciones. Si es necesario, hardware puede adquirirse por el cliente en función de las especificaciones proporcionadas por nosotros.

Operadores de Terminales

Los operadores de las terminales son unidades estándar de escritorio, con las siguientes especificaciones:

- Procesador: Core i5
- Memoria: 3 GB de RAM

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental Lineamiento Décimo Octavo fracción II y V, inciscos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

- Disco Duro: 320 GB
- Sistema operativo: Windows 7

Sistema de Hardware

Para apoyar plenamente la infraestructura del sistema, el siguiente hardware se requiere:

- Dos unidades de 42U gabinete
- Redes hardware
- 10TB de almacenamiento
- 5 servidores estándar
- UPS
- Celular módems y tarjetas SIM

GARANTÍA, MANTENIMIENTO Y ACTUALIZACIONES DE "EL BIEN"

La garantía de **"EL BIEN"** será de 12 meses a partir de la fecha de recepción del mismo. **"EL PROVEEDOR"** se compromete a proporcionar mantenimiento a **"EL BIEN"** y brindar soporte, sin costo para **"LAPROCURADURÍA"** de conformidad a lo siguiente:

Mantenimiento y Soporte

"EL PROVEEDOR" proporcionará servicios de mantenimiento y soporte de nivel tres niveles que incluye:

- **Nivel 1:** Sistema estándar operaciones problemas de correo electrónico y soporte telefónico
- **Nivel 2:** Resolución proactiva de ingenieros dedicados problemas o técnica inspeccionará, examinar y resolver problemas técnicos comunes, poniendo sus mejores esfuerzos, asistencia remota usando software de escritorio remoto y una red privada Virtual (VPN) cuando así lo solicite
- **Nivel 3:** Fallo sistema de fijación y las actualizaciones de sistema importantes desperfectos

Soporte telefónico: además de lo anteriormente mencionado, **"EL PROVEEDOR"** proporciona el teléfono y correo electrónico para cualquier pregunta y solución de algún el problema.

Además, "EL PROVEEDOR" será capaz de añadir la siguiente asistencia

- Asistencia en el sitio planeado o de emergencia
- Sistema de monitoreo de salud

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

COTIZACIÓN EXPEDIDA POR "EL PROVEEDOR" DE FECHA 24 DE OCTUBRE DE 2014.

Introducción

Pegasus es una solución de inteligencia líder en el mundo cibernético que permite la aplicación de la ley y las agencias de inteligencia que remotamente y secretamente extraen inteligencia valiosa desde prácticamente cualquier dispositivo móvil. Esta solución innovadora fue desarrollada por los veteranos de las agencias de inteligencia de élite para proporcionar a los gobiernos con una forma de abordar los nuevos desafíos de interceptación de comunicaciones en batalla cibernética altamente dinámica de hoy. Mediante la captura de nuevos tipos de información desde dispositivos móviles, Pegasus es un desfase tecnológico sustancial que ofrece la más completa y precisa inteligencia para sus operaciones de seguridad.

Desafío de Intercepción de Smartphone

El mercado de las comunicaciones móviles altamente dinámico y creciente - caracterizado por la introducción de nuevos dispositivos, sistemas operativos y aplicaciones prácticamente a diario – exige un replanteamiento del paradigma tradicional de la inteligencia. Estos cambios en el paisaje de comunicaciones plantean verdaderos desafíos y obstáculos que deben ser superados por las organizaciones de inteligencia y policiales en todo el mundo:

- Cifrado: Amplia utilización de dispositivos encriptados y aplicaciones para transmitir mensajes
- Abundancia de aplicaciones de comunicación: caótico mercado de aplicaciones sofisticadas, más de las cuales son basadas en IP y usar protocolos propietarios.
- Objetivo fuera interceptación dominio: Comunicaciones objetivos son a menudo fuera del dominio de interceptación de la organización u otra manera inaccesibles (por ejemplo, los objetivos son itinerantes, cara a cara reuniones, uso de redes privadas, etc.)
- Enmascaramiento: Uso de diferentes identidades virtuales que son casi imposibles de reemplazo de SIM.
- Seguimiento y Rastreo: Reemplazo de tarjetas SIM para evitar cualquier tipo de extracción de datos.
- Interceptación Frecuente: La mayoría de la información no se envían a través de la red o compartida con otros partidos y sólo está disponible para el usuario final dispositivo.
- Compleja y Costosa Implementación: Como las comunicaciones se convierten cada vez más complejas, son necesarios más interfaces de red. Configurar estas interfaces con los proveedores de servicio es un proceso largo y costoso y requiere de regulación y normalización.

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Soluciones estándar de interceptación no son suficientes

Hasta que se abordan los desafíos mencionados y objetivos resueltos, criminales y terroristas son probablemente es "seguro" de sistemas estándar y el legado de interceptación, lo que significa que se está perdiendo valiosa inteligencia. Estas soluciones estándar (descritas en las secciones a continuación) entregan sólo parcial inteligencia, dejando a las organizaciones con boquetes de inteligencia substancial.

Intercepción Pasiva

Intercepción pasiva requiere muy profundas y estrecha relaciones con proveedores de servicios locales (celulares, proveedores de Internet y PSTN) y tradicionalmente ha permitido para un seguimiento adecuado de los mensajes de texto y llamadas de voz. Sin embargo, la comunicación más contemporánea se compone de tráfico basadas en IP, que es extremadamente difícil de controlar con intercepción pasiva debido a su uso de cifrado y protocolos propietarios.

Aun cuando este tráfico es interceptado, típicamente lleva cantidades masivas de datos técnicos que no están relacionados con el contenido real y los metadatos se comunican. No sólo tiene este resultado en analistas frustrados y tiempo perdido en circular a través de datos irrelevantes, también proporciona una reproducción parcial (la mejor) de las comunicaciones del objetivo. Además, el número de interfaces requeridas para cubrir los prestadores de servicios pertinentes amplía el círculo de entidades expuestas a información sensible y aumenta la posibilidad de fuga.

Intercepción Táctica GSM

Soluciones tácticas de interceptación GSM monitorizan de manera efectiva las llamadas de voz y mensajes de texto en las redes GSM. Cuando avanzadas tecnologías celulares son desplegados (Redes 3G y LTE), estas soluciones se vuelven menos eficientes. En tales casos, es necesario rebajar violentamente el objetivo de una red basada en GSM, que afecta notablemente la experiencia del usuario y la funcionalidad

Estas soluciones también requieren de un equipo táctico bien entrenado y un campo situado cerca del objetivo monitoreado. Así, en la mayoría de los casos donde se desconoce la ubicación de destino, estas soluciones convertidas en irrelevantes. En otros casos, colocando un equipo táctico cerca del objetivo puede plantear grave riesgo al equipo y a la operación de inteligencia entera.

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014"*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Software Malicioso (Malware)

Malware presumiblemente proporciona acceso al dispositivo móvil del objetivo. Sin embargo, no es completamente transparente y requiere la implicación del objetivo para ser instalado en sus dispositivos. Este tipo de compromiso generalmente toma la forma de múltiples confirmaciones y aprobaciones antes de que el malware sea funcional. La mayoría de los blancos es poco probable que se deje engañar para que coopere con malware debido a su alto nivel de sensibilidad para la privacidad en sus comunicaciones.

Además, tal malware es probable ser vulnerable a la mayoría de software anti-spyware y antivirus disponible comercialmente. Como tal, dejan rastros y son fácilmente detectados en el dispositivo.

Inteligencia Cibernética para el Mundo Móvil

Pegasus es una solución de inteligencia líder en el mundo cibernético que permite la aplicación de la ley y las agencias de inteligencia que remotamente y secretamente extraer inteligencia valiosa desde prácticamente cualquier dispositivo móvil. Esta solución innovadora fue desarrollada por los expertos de las agencias de inteligencia de élite para proporcionar a los gobiernos con una forma de abordar los nuevos desafíos de interceptación de comunicaciones en batalla cibernética altamente dinámica de hoy.

Mediante la captura de nuevos tipos de información desde dispositivos móviles, Pegasus puentes un desfase tecnológico sustancial para ofrecer la más completa y precisa inteligencia para sus operaciones de seguridad. Esta solución es capaz de penetrar los smartphones más populares del mercado basados en sistemas operativos BlackBerry, Android, iOS y Symbian.

Pegasus silenciosamente implementa software invisible ("agente") en el dispositivo de destino. Este agente luego extractos y transmite correctamente los datos recogidos para su análisis. Instalación se realiza de forma remota (OTA), no requiere ninguna acción de o compromiso con el objetivo y no deja ningún rastro alguno en el dispositivo.

Beneficios de Pegasus

Organizaciones que desplegar Pegasus son capaces de superar los retos mencionados para lograr la recolección de inteligencia móvil incomparable:

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Acceso ilimitado a los dispositivos móviles del objetivo: Remotamente y secretamente recopilar información sobre de su objetivo relaciones, ubicación, llamadas telefónicas, planes y actividades – cuando y donde son.

Interceptar llamadas: Seguimiento transparente de voz y llamadas VoIP en lagunas de inteligencia en tiempo real.

- Puente: **Recoger únicos y nuevos tipos de información (ej. Contactos, archivos, vigilancia ambiental, contraseñas, etc...) para ofrecer la más completo y preciso inteligencia.**
- Mango codificado contenido y dispositivos: **Superar la encriptación, SSL, protocolos propietarios y cualquier obstáculo presentado por el monitoreo de aplicaciones complejas comunicaciones mundial.**
- Monitorear una multitud de aplicaciones: **Incluyendo objetivos como: Skype, WhatsApp, Viber, Facebook y BlackBerry Messenger (BBM).**
- Seguimiento de objetivos: **Obtener información utilizando independencia GPS**
- Servicio proveedor de posicionamiento preciso: **No cooperación con la red móvil local los operadores (MNO) es necesario.**
- Descubrir identidades virtuales: **Monitorear constantemente el dispositivo sin preocuparse de conmutación frecuente de identidades virtuales y reemplazo de tarjetas SIM.**
- Evite riesgos innecesarios: **Eliminar la necesidad de proximidad física con el objetivo o el dispositivo en cualquier fase.**

Tecnología Destacada

La solución de Pegasus utiliza tecnología de punta especialmente desarrollada por veteranos de inteligencia y policiales. Ofrece un rico conjunto de características avanzadas y las capacidades de inteligencia sofisticada colección no están disponibles en las soluciones estándar de intercepción:

- **Penetra en Android, BlackBerry, iOS y dispositivos basados en Symbian**
- **Acceso a dispositivos protegidos por contraseña**
- **Totalmente transparente para el objetivo**
- **No deja huella en el dispositivo**
- **Mínima batería, memoria y datos consumo**
- **Autodestrucción en caso de exposición riesgo**
- **Recupera cualquier archivo desde el dispositivo para análisis más profundo**

Arquitectura de Alto Nivel

El sistema Pegasus está diseñado en capas. Cada capa tiene la responsabilidad de formar juntos una solución de análisis y recolección de inteligencia cibernética integral.

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Las capas principales y bloques de construcción de los sistemas son:

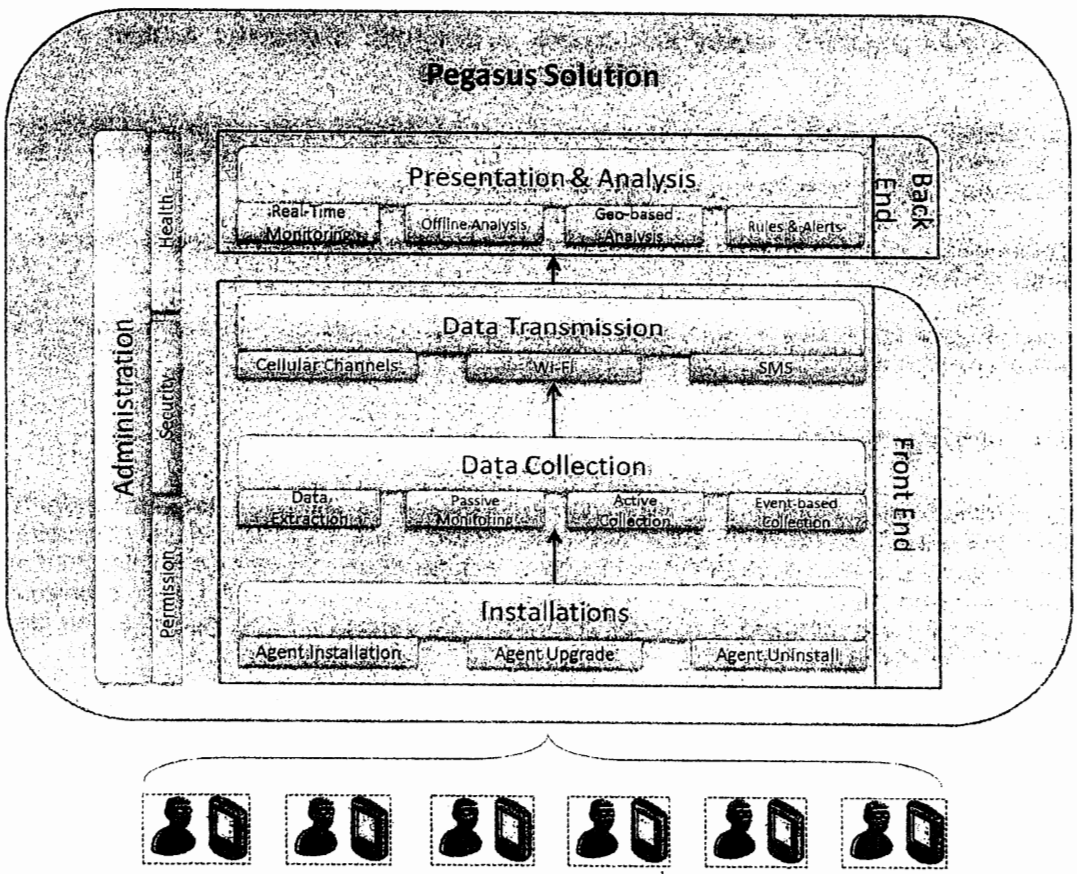
- Instalaciones: **Capa de la instalación está a cargo de la emisión de las nuevas instalaciones de agente, actualizar y desinstalar agentes existentes.**
- Recolección de datos: **Capa de la recopilación de datos está a cargo de recoger los datos desde el dispositivo instalado. Pegasus ofrece inteligencia integral y completa mediante el empleo de métodos de recolección de cuatro**
- Extracción de datos: **Extracción de los datos todo que existe en el dispositivo sobre la instalación del agente**
- Vigilancia pasiva: **Nuevos datos de llegada al dispositivo**
- Colección Monitor Activo: **Activar la cámara, micrófono, GPS y otros elementos para recopilar datos en tiempo real**
- Colección basada en eventos: **Definir escenarios que activa automáticamente datos específicos colección**
- Transmisión de datos: **La capa de transmisión de datos es la encargada de transmitir los datos a los servidores de comando y control, utilizando la forma más eficiente y segura.**
- Análisis de la presentación: **El componente de presentación análisis es una interfaz de usuario que se encarga de presentar los datos recogidos a los operadores y analistas, convirtiendo los datos de inteligencia. Esto se hace mediante los siguientes módulos:**
- Monitoreo en tiempo real: **Presenta los datos recogidos en tiempo real de específico o varios objetivos. Este módulo es muy importante cuando se trata de objetivos sensibles o durante las actividades operacionales, donde cada pieza de información que llega es crucial para la toma de decisiones.**
- Análisis offline: **Avanzado mecanismo de consultas que permite a los analistas consultar y recuperar cualquier pieza de información que se recopila. El mecanismo avanzado proporciona herramientas para encontrar información y conexiones ocultas.**
- Análisis basado en geolocalización: **presenta los datos recogidos en un mapa y conducta consultas basadas en geo.**
- Administración: **es el componente de administración encargado de gestionar el permiso de todo el sistema, seguridad y salud: contactos de extractos mensajes, correos electrónicos, fotos, archivos, ubicaciones, contraseñas, lista de procesos y más**
- Permiso: **el mecanismo de permisos permite al administrador del sistema gestionar los distintos usuarios del sistema. Proporcionar cada uno de ellos el nivel correcto acceso sólo a los datos que se les permite. Esto permite para definir los grupos de la organización que manejan sólo uno o más temas y otros grupos que maneja diferentes temas.**
- Seguridad: **El módulo de seguridad monitorea el nivel de seguridad del sistema, asegurándose de que los datos recogidos se insertan a la base de datos de sistema limpio y seguro para su futura revisión.**
- Salud: **El componente de salud de la solución de Pegasus monitorear el estado de todos los componentes asegurándose de que todo está funcionando sin problemas. Monitorea la comunicación entre las diferentes partes, el rendimiento del sistema, la disponibilidad de almacenamiento de información y alertas si algo falla.**

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, (incisos c) y d)) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

Las capas del sistema y los componentes se muestran en la figura 1.

Figura 1: Arquitectura de nivel alto de Pegasus



PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Instalación del Agente

Para empezar a recolectar datos desde smartphone su blanco, un componente de software de base ("agente") debe de forma remota y secretamente instalarse en su dispositivo.

Propósito del Agente

El "agente", un componente de software base, reside en los dispositivos de punto final de las metas monitoreadas y su propósito es reunir los datos para que se configuró. El agente es compatible con los sistemas operativos más populares: dispositivos basados en Symbian, BlackBerry, Android y iOS (iPhone).

Cada agente es independiente y está configurado para recolectar información diferente del dispositivo y para transmitir la señal mediante canales específicos en plazos definidos. Los datos se envían a los servidores de Pegasus de manera oculta, comprimida y encriptada.

El agente continuamente recopila la información del dispositivo y lo transmitirá una vez que disponga de conexión a internet confiable.

Cifrado de las comunicaciones, el uso de muchas aplicaciones y otras comunicaciones ocultar métodos ya no es relevantes cuando un agente está instalado en el dispositivo.

Vector de Instalación del Agente

Inyectables y la instalación de un agente en el dispositivo son la fase más sensible e importante de la operación de inteligencia llevada a cabo en el dispositivo de destino. Cada instalación debe planearse con cuidado para asegurar que tiene éxito. El sistema Pegasus soporta varios métodos de instalación. La variedad de métodos de instalación responde a los distintos escenarios operacionales que son únicos para cada cliente, dando como resultado la solución más completa y flexible. Los siguientes son los vectores de instalación admitidos:

Instalación Remota (Rango):

- Por aire (OTA): empuje se envía un mensaje de forma remota y secretamente en el dispositivo móvil. Este mensaje activa el dispositivo para descargar e instalar al agente en el dispositivo durante toda la instalación proceso de cooperación o compromiso del objetivo se requiere (por ejemplo, hacer clic en un vínculo, un mensaje de apertura) y ninguna indicación aparece en el dispositivo. La instalación es totalmente silencioso e invisible y no puede ser prevenida por el objetivo. Esta es la singularidad NSO, que distingue significativamente la solución Pegasus de cualquier otra solución disponible en el mercado.

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*"Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental, Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

- **Mensaje de ingeniería Social mejorado (ESEM):** En casos donde el método de instalación OTA es inapplicable1, el operador del sistema puede elegir enviar un mensaje de texto normal (SMS) o un correo electrónico, atrayendo el objetivo para abrirlo. Solo clic, planificada o no intencional, en el enlace se traducirá en instalación del agente oculto. La instalación está totalmente oculta y aunque el objetivo hacer clic en el enlace no serán conscientes de que software está siendo instalado en su dispositivo.

Las posibilidades de que el objetivo se haga clic en el enlace son totalmente dependientes en el nivel de contenido credibilidad. La solución de Pegasus ofrece una amplia gama de herramientas para componer un mensaje inocente y diseñado para atraer la meta para abrir el mensaje.

Nota: Ambos métodos OTA y ESEM requieren solamente un número de teléfono o una dirección de correo electrónico que se utiliza por el objetivo. Nada más se necesita para lograr una instalación exitosa del agente Pegasus en el dispositivo

Cerca del objetivo (Rango limitado):

- **Elemento táctico de red:** agente de la Pegasus puede ser inyectado en silencio una vez que el número se adquiere mediante el elemento de red táctica como **Base estación transmisora** (BTS). El Pegasus la solución aprovecha las capacidades de estas herramientas tácticas para llevar a cabo una inyección remota e instalación del agente. Tomando una posición en el área de la blanco es, en la mayoría de los casos, suficientes para llevar a cabo la adquisición de número de teléfono. Una vez que el número está disponible, la instalación se realiza remotamente.

- **Física:** cuando el acceso físico al dispositivo es una opción, el agente de Pegasus puede ser manualmente inyectado e instalado en menos de cinco minutos. Después de la instalación del agente, extracción de datos y monitoreo de datos futuros se realiza remotamente, ofreciendo las mismas características de cualquier otro método de instalación.

Nota: Generalmente se utilizan instalaciones Tácticas y físicas donde ningún número de teléfono de destino o dirección de correo electrónico están disponibles.

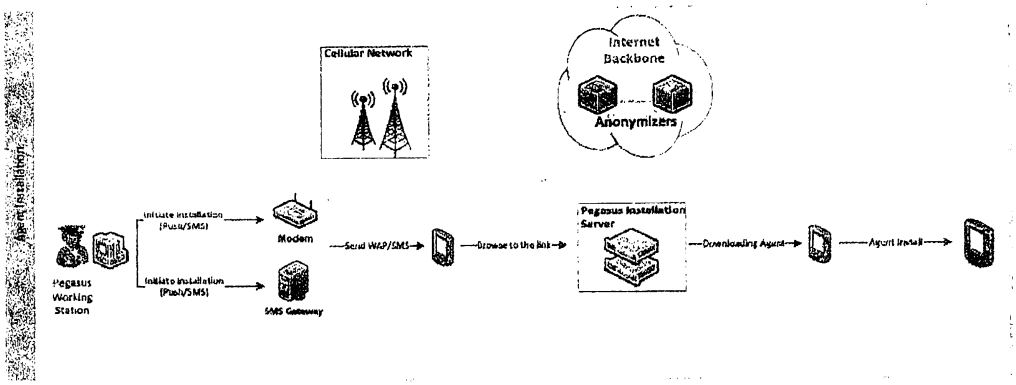
PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Flujo de instalación del agente

Flujo de instalación del agente remoto se muestra en la Figura 2.

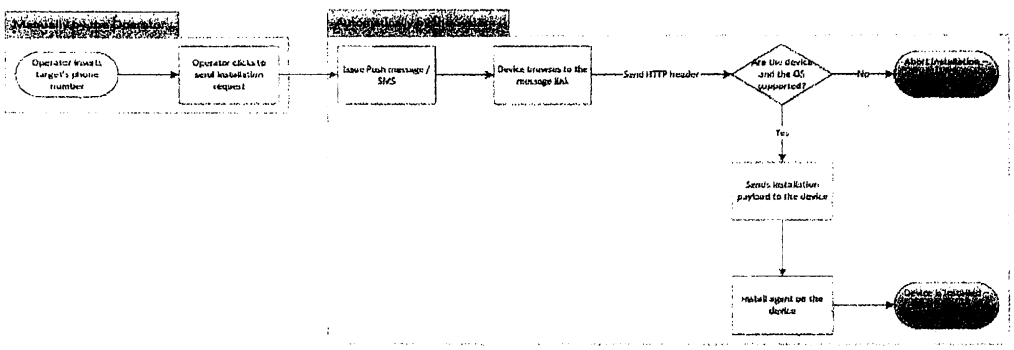
Figura 2: Flujo de instalación del agente



Para iniciar una nueva instalación, el operador del sistema Pegasus sólo debe introducir el número de teléfono de destino. El resto se realiza automáticamente por el sistema, resultando en la mayoría de los casos con un agente instalado en el dispositivo de destino

Iniciación de configuración del agente se muestra en la Figura 3.

Figura 3: El Agente de inicio de instalación



PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Sistemas y Dispositivos Operativos Compatibles

Sistema Operativo (SO)	Versión OS	Dispositivo	Comentarios
Android	2.1 - 4.2	Samsung Galaxy series Sony Ericsson Xperia series Otros	El apoyo se basa en las versiones locales de firmware, cosa que se debe definir con el cliente.
iOS	4.x - 6.1.4	iPhone 4 iPhone 4S iPhone 5	
BlackBerry	5.0 - 7.1	Curve (8520, 9300, 9350,9360) Bold (9000,9700, 9780, 9790, 9900, 9930) Torch (9800, 9810, 9850, 9860) Pearl (9100)	
Symbian	Versión S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variedad de dispositivos	El apoyo se basa en las versiones locales de firmware, cosa que se debe definir con el cliente.

Nota: Los dispositivos basados en Android a menudo se añaden a la lista de admitidos. Una lista actualizada puede ser enviada a petición del cliente.

Falló la instalación la instalación:

A veces puede fallar debido a las razones siguientes:

1. **Dispositivo no compatible**: el dispositivo de destino no es compatible con el sistema (que aparece más arriba).
2. **Sin soporte OS:** el sistema operativo del dispositivo de destino no es compatible con el sistema
3. **Sin soporte de navegador:** el navegador por defecto del dispositivo previamente fue reemplazado por el objetivo. Instalación de los navegadores distinta de la predeterminada del dispositivo (y también dispositivos basados en Chrome para Android) no es compatible con el sistema.

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

En cualquiera de los casos antes mencionados, si el operador inicia una instalación remota a un dispositivo no compatible, sistema operativo o navegador, la inyección se producirá un error y se aborta la instalación. En estos casos el proceso haya terminado con un navegador abierto en el dispositivo de destino apuntando y mostrando la página URL que fue definida por el operador antes de la instalación. El dispositivo, el sistema operativo y el navegador se identifican mediante el sistema mediante su agente de usuario HTTP. Si por algún motivo que el agente de usuario fue manipulado por el blanco, el sistema podría no identificar correctamente el dispositivo y el sistema operativo y proporcionan la carga instalación incorrecta. En tal caso, la inyección se producirá un error y se aborta la instalación, mostrando nuevamente la página URL antes mencionada.

Recolección de Datos

Tras la instalación del agente exitoso, una amplia gama de datos se controla y recopilada desde el dispositivo:

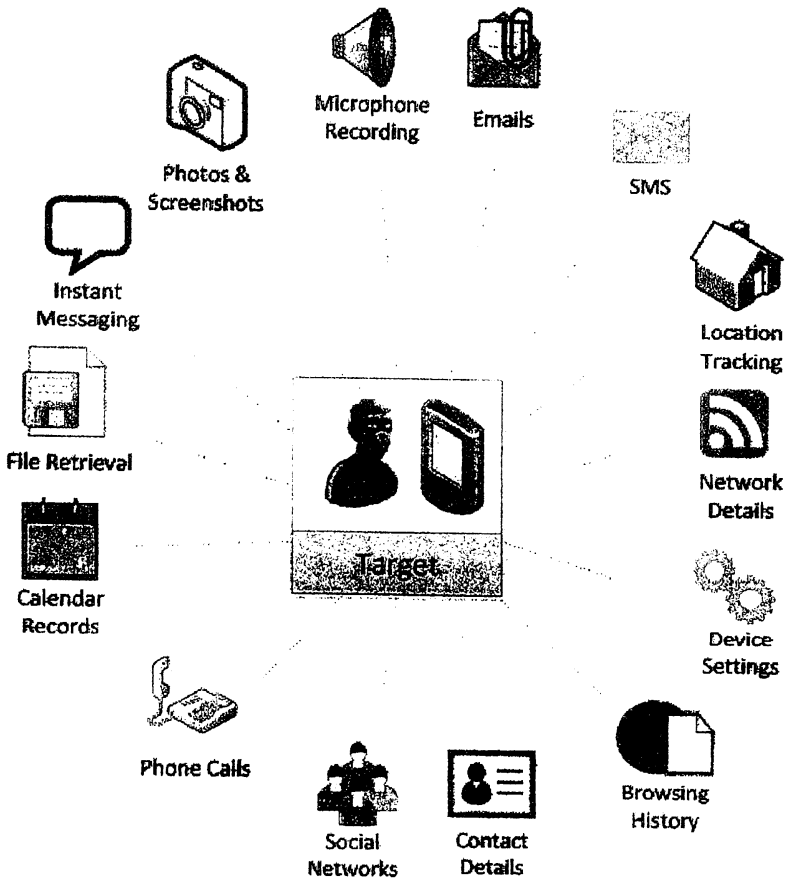
- **Textual:** Información Textual incluye mensajes de texto (SMS), correos electrónicos, registros de calendario, llamado historia, mensajería instantánea, lista de contactos, viendo la historia y mucho más. Información textual suele ser estructurado y pequeño de tamaño, por lo tanto más fácil de transmitir y analizar.
- **Audio:** Audio información incluye llamadas interceptadas, sonidos ambientales (grabación de micrófono) y otros archivos de audio grabados.
- **Visual:** información Visual incluye cámaras instantáneas, recuperación de fotos y capturas de pantalla.
- **Archivos:** cada dispositivo móvil contiene cientos de archivos, algunos osos inteligencia invaluable, tales como bases de datos, documentos, videos y más.
- Ubicación: seguimiento de la ubicación del dispositivo (Cell-ID y GPS) continúa

La variedad de los datos que son recogidos por el sistema Pegasus se muestra en la Figura 4.

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*"Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

Figura 4: Los datos Recopilados.



La recolección de datos se divide en tres niveles:

- Extracción Inicial
- Monitoreo Pasivo
- Recolección de Datos Activa

PGR
PROCURADURIA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Extracción Inicial de Datos

Una vez que el agente es inyectado con éxito e instalado en el dispositivo, los siguientes datos que residen y que existen en el dispositivo pueden extraerse y enviados al centro de mando y control

- **Registro de SMS**
- **Detalle de Contactos**
- **Historial de Llamadas (registro)**
- **Calendario de registros**
- **Mensaje de Correo Electrónico**
- **Mensajería instantánea**
- **Historial de Navegación**

A diferencia de otras soluciones de colección de inteligencia que proporcionan sólo futuro monitoreo de comunicaciones parciales, Pegasus permite la extracción de todos los datos existentes en el dispositivo. Como resultado la organización goza de acceso a datos históricos sobre el objetivo, que asiste en la construcción de una imagen completa y precisa de la inteligencia.

Nota: La extracción de datos inicial es una opción y no una necesidad. Si la organización no está permitida acceder a los datos históricos del blanco, esta opción puede desactivarse y sólo nuevos datos de llegada serán monitorizados por el agente

Monitoreo Pasivo

Desde el punto del que agente fue instalado con éxito mantiene el dispositivo de monitoreo y recupera cualquier nuevo registro que esté disponible en tiempo real (o en condición específica si configura diferentemente). Debajo está la lista completa de datos que es supervisado por el agente:

- Registros de SMS
- Detalles de Contactos
- Historial de llamadas (Registro)
- Calendario de Registros
- Mensajes de correo electrónico
- Mensajería instantánea
- Historial de navegación
- Ubicación de Seguimiento (Cell-ID basada)

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*Fecha de la clasificación	México, D.F., a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

Recopilación activa

Además de la vigilancia pasiva, Al exitoso agente de instalar el amplio conjunto de colección esté disponible. Colección activa se refiere a activar las solicitudes enviadas por los operadores para recoger información específica del unscrew instalado. Este conjunto de características son llamada activa, llevan su cum colección implícita A solicitud del explotador. Activo colección permite al operador realizar las acciones en tiempo real sobre la recuperación de dispositivos de destino información única del dispositivo y de los alrededores de la meta, que incluye:

- Rastreo de ubicación (basado en el GPS)
- Las llamadas de voz intercepción
- Recuperación de archivos
- Grabación de sonido ambiental (Grabación de micrófono)
- Seguimiento de fotos
- Captura de Pantalla

Colección activa distingue a Pegasus de cualquier otra solución de colección de inteligencia, como el operador controla la información que se recopila. En lugar de sólo esperando información llegar, esperando que esta es la información que buscas, el operador activamente recupera información importante desde el dispositivo, recibiendo la información exacta que estaba buscando.

Descripción de los datos recogidos.

Los diferentes tipos de datos disponibles para la extracción, vigilancia pasiva y activa colección con sus respectivas características se enumeran en la tabla 1.

PGR
PROCURADURIA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F. a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencias y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Tabla 1: Descripción de las Características de la Colección

Tipo de Aplicación	Descripción de Características	Extracción de Datos	Colección Pasivo/Activo
Mensajeria Instantánea: 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	El agentes extrae y monitorea todos los mensajes instantáneos entrantes y salientes a / desde el dispositivo. Extracción 1 contra 1 en conversación y seguimiento incluyendo grupo de chat. Indicación para la transferencia de archivos (nombre del archivo).	*	*
Seguimiento de la ubicación	El sistema proporciona dos tipos de información de ubicación acerca del dispositivo: <u>GPS:</u> 1. A petición del usuario, se abre un plazo de tiempo definido para la zona de muestreo. Se recuperan los datos GPS en su caso (la recepción está disponible). En caso de no se recupera accesible, Cell-ID de la señal GPS. 2. Si el GPS está desactivado por el blanco, el sistema permite que para el muestreo e inmediatamente apagarlo. <u>Cell-ID:</u> Los dispositivos constantemente transmiten su ubicación (Cell-ID) cada vez que se comunican con el servidor. Los datos de ubicación recuperada se analizan en el servidor y se coloca en el mapa. Las consultas y alertas basadas en la localización se fijan fácilmente.	*	*
Calendario	El agente extrae todos los registros de calendario desde el dispositivo y monitorea cualquier cambio o nuevo evento añadido al calendario.	*	*
Detalles de Contacto	El agente extrae todos los contactos disponibles en el dispositivo. De esta manera el agente monitorea cualquier cambio / eliminación de los contactos existentes y la adición de nuevos contactos. El agente extrae y supervisa todos los valores asignados en cada campo de contacto que está disponible (basado en campos vCard), incluyendo la foto si se ha asignado.	*	*

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*"Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

Tipo de Aplicación	Descripción de Características	Extracción de Datos	Colección Pasivo /Activo
Grabación de sonido ambiental (grabación del micrófono)	El usuario puede solicitar para encender el micrófono del dispositivo y escuchar en tiempo real a los sonidos del entorno. Los sonidos del entorno se registran y pueden ser analizados y reproducidos en una etapa posterior. Al encender el micrófono se basa en una llamada silenciosa en el dispositivo desde el servidor (PBX). Se autorizará dicha llamada sólo después de que el agente de seguridad de que el dispositivo está en modo de reposo (el dispositivo no está en uso activo y la pantalla está apagada). Ninguna acción de la meta que se enciende la pantalla dará lugar a la llamada inmediata de colgar y de cese de la captura de los sonidos del entorno. No hay indicación de la grabación o la llamada silenciosa entrante aparece en el dispositivo, en cualquier punto. La calidad de la grabación depende de la sensibilidad del micrófono del dispositivo, el ruido circundante y el modelo del dispositivo. Esta sensibilidad varía entre los diferentes modelos de teléfonos móviles y es fijado por el fabricante del teléfono. Por lo general, el contenido de una conversación celebrada a pocos metros al lado del dispositivo puede ser escuchado.	N/A	*
SMS	El agente extrae y monitorea todos los mensajes de texto entrantes y salientes (SMS).	*	*
Intercepción de Llamada (Grabación de llamada) - Solo Android	El usuario puede pedir grabar llamadas entrantes y salientes del dispositivo del objetivo. Las llamadas son grabadas localmente en el dispositivo y después enviadas al servidor hasta que se complete.	N/A	*
Email: 1. Aplicación de Email en todas las plataformas. 2. Aplicaciones Gmail en Android	Agente extrae y supervisa todos los correos electrónicos que se encuentran en el dispositivo. La aplicación de correo electrónico principal (acción) en el dispositivo se controla, por lo tanto, todas las cuentas que se definen no son monitoreados (por ejemplo, el intercambio, gmail, etc.) Para dispositivos basados en Android tanto en la aplicación de correo electrónico principal y la aplicación gmail son monitoreadas.	*	*
Recuperación de archivos	A petición del usuario una lista completa de los archivos y carpetas se extrae del dispositivo (memoria interna y la tarjeta SD). Cuando el operador ve un archivo de interés que puede solicitar de inmediato para recuperarlo.	N/A	*

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Toma de la foto	Al usuario de petición instantánea utilizando la cámara frontal y trasera se toman desde el dispositivo y se envían a los servidores. Se toman las instantáneas después de que el agente de seguridad de que el dispositivo está en modo inactivo. Durante la foto teniendo la indicación aparece en el dispositivo y el flash no se utiliza nunca. La calidad de la foto puede ser elegida por el operador para reducir el uso de los datos y la transmisión rápida de fotos. Dado que el flash no se utiliza y el teléfono podría estar en movimiento o las habitaciones interiores con poca luz, las fotos son a veces fuera de foco.	N/A	*
Captura de Pantalla	A petición del usuario se toma una captura de pantalla y se envía a los servidores de Pegasus. Las capturas de pantalla de dispositivos pueden proporcionar información sobre las aplicaciones utilizadas por el objetivo, imagen de fondo utilizada y la información más íntima sobre el objetivo.	N/A	*
Historial de navegación	El agente extrae y monitorea el historial de los sitios web explorados desde el navegador predeterminado del dispositivo.	*	*
Favoritos de navegación	Los agentes extraen y monitorean los sitios web favoritos guardados en el navegador predeterminado del dispositivo.	*	*
Historial de llamadas	El agente extrae el historial de todas las llamadas entrantes / salientes realizadas desde / hacia el dispositivo. Los datos incluyen la persona que llama y los números llamados y la duración de la llamada. Intentos que no resultaron con una conversación de llamada mostrará la duración de 0 (cero) segundos.	*	*
Historial de llamadas	El agente extrae el historial de todas las llamadas entrantes / salientes realizadas desde / hacia el dispositivo. Los datos incluyen la persona que llama y los números llamados y la duración de la llamada. Intentos que no resultaron con una conversación de llamada mostrará la duración de 0 (cero) segundos.	*	*

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F. a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"(sic)*
Rúbrica del Titular de la Unidad Administrativa	

Los datos antes mencionados son los datos posibles que pueden ser recolectados por un agente. El agente recopilará los datos que están disponibles en el dispositivo y aplicables. Si no existe uno o más de las aplicaciones mencionadas o quitado el dispositivo, el agente funcionará de la misma manera. Recolectarán los datos del resto de los servicios y aplicaciones que están en uso en el dispositivo. Además, todos los datos recogidos desde la aplicación quitado todavía se guardarán en los servidores o en el agente, si no era todavía transmiten a los servidores.

Además, los datos antes mencionados que son recogidos por el agente cubren las aplicaciones más populares utilizadas en el mundo. Puesto que la popularidad de las aplicaciones varía de país a país, que entiende la extracción de datos y monitoreo de aplicaciones será necesarios tiempo evoluciona y nuevas aplicaciones son adoptadas por objetivos. Cuando tal requisito se levanta, podemos fácilmente extraer datos importantes de prácticamente cualquier aplicación basada en la demanda del cliente y lanzarlo como una nueva versión que estará disponible para el cliente.

Colección de Buffer

El agente instalado monitorea los datos desde el dispositivo y la transmite a los servidores. Si la transmisión no es possible3 el agente recogerá la nueva información disponible y la transmite cuando se disponga de conexión. Los datos recogidos se almacenan en un búfer oculto y cifrado. Este buffer está listo para llegar a no más del 5% del espacio libre disponible en el dispositivo. Por ejemplo, si el dispositivo monitoreado tiene 1GB de espacio libre, el buffer puede almacenar hasta 50MB. En caso de que el buffer ha llegado a su límite, los datos más antiguos se borran y se almacenan los datos nuevos (FIFO). Una vez que se ha transmitido los datos, el contenido del búfer es totalmente eliminado.

Transmisión de Datos

De forma predeterminada, los datos recogidos (extracción de los datos iniciales, vigilancia pasiva y activa colección) son enviados hacia el centro de comando y control en tiempo real. Los datos se envían a través de canales de datos, donde Wi-Fi es la conexión preferida para utilizar cuando está disponible. En otros casos se transmiten datos mediante canales de datos móviles (GPRS, 3G y LTE). Extra pensaba poner en métodos de compresión y centrarse en la transmisión de contenido textual siempre que sea posible. Las huellas de datos son muy pequeñas y suelen tener sólo unos cientos de bytes. Esto es para asegurarse de que los datos recogidos se transmiten fácilmente, asegurando un impacto mínimo en el dispositivo y en el plan de datos móviles de blanco.

Si no existen canales de datos, el agente de recopilar la información del dispositivo y guárdela en un búfer dedicado, como se explica en la sección de recopilación de datos.

Transmisión de datos es cesada automáticamente en los siguientes escenarios:

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

- **Batería baja**: cuando el nivel de la batería del dispositivo está por debajo del umbral definido (5%) todos los procesos de transmisión de datos son cesó inmediatamente hasta que el dispositivo está recargado.

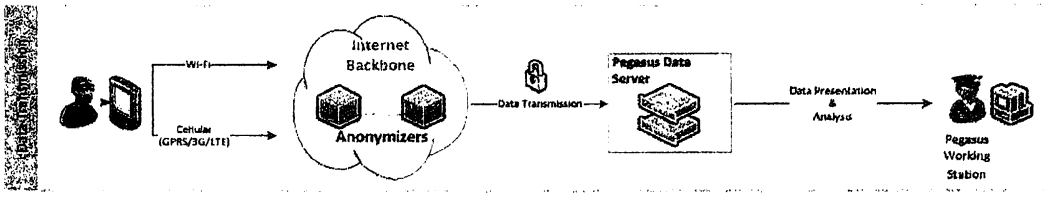
- **Dispositivo Roaming**: cuando el dispositivo está en roaming, se convierten en canales de datos celulares caros, por lo tanto la transmisión de datos se realiza sólo a través de Wi-Fi. Si no existe conexión Wi-Fi, la transmisión será cesada.

Cuando no hay canales de datos están disponibles, y ninguna indicación para la comunicación va a volver desde el dispositivo, el usuario puede solicitar el dispositivo se comunica o enviar algunos datos cruciales usando mensajes de texto (SMS).

PRECAUCIÓN: Transmisión de comunicación y/o datos vía SMS puede incurrir en costos por el objetivo y aparecen en su facturación informe así debe ser usado con moderación.
La comunicación entre el agente y los servidores centrales es indirecta (a través de la red de anonimato), así que se remontan al origen es no-factible.

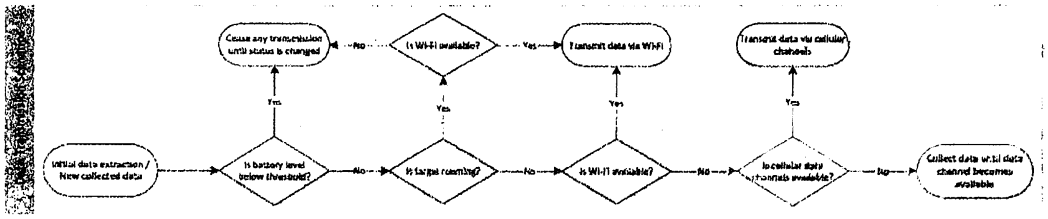
El proceso de transmisión de datos de sistema Pegasus se muestra en la figura 5.

Figura 5: Proceso de transmisión de datos



Los canales y escenarios para la transmisión de los datos recogidos se muestran en la figura 6.

Figura 6: Escenarios de transmisión de datos



PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F. a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Seguridad de la Transmisión de Datos

Todas las conexiones entre los agentes y los servidores están cifradas con algoritmos fuertes y mutuamente se autentican. Cifrado de datos es probablemente el tema más instando a, cuidado adicional fue dado para asegurar la memoria, pila y datos mínimos son consumidos dentro de los requerimientos de los agentes. Esto es para asegurarse de que no se crían preocupación por el destino. Es casi imposible detectar a un agente operativo por el objetivo. El agente Pegasus está instalado a nivel del núcleo del dispositivo, bien ocultado y es imposible de encontrar por el software antivirus y anti-espía.

Los datos transmitidos están encriptados con cifrado simétrico AES de 128 bits.

Red de Transmisión Anónima de Pegasus

Agente transparencia y seguridad de la fuente son los principios rectores de la solución de Pegasus. Para asegurar que se remontan a la entidad explotadora es imposible, el Pegasus anonimizar transmisión Network (red), una red de Anonimizadores se despliega para servir a cada cliente. Los nodos de la red se distribuyen en diferentes lugares alrededor del mundo, permitiendo a agente conexiones ser redirigido a través de diferentes caminos antes de llegar a los servidores de Pegasus. Esto asegura que las identidades de ambas partes comunicantes son altamente oscurecidas.

Presentación de Datos y Análisis.

Recopilación de datos exitoso de cientos de objetivos y dispositivos genera enormes cantidades de datos para análisis, presentación y visualización. El sistema proporciona un conjunto de herramientas operativas para ayudar a la organización a transformar datos de inteligencia. Esto es para ver, ordenar, filtrar, consultar y analizar los datos recogidos. Las herramientas incluyen:

- **Análisis Geográfico**: seguimiento de localización en tiempo real e históricos del objetivo, varios objetivos en el mapa
- **Reglas y alertas:** definir reglas para generar alertas a la llegada de los datos importantes
- **Favoritos:** marcar eventos importantes y favoritos para revisión posterior y más profundo análisis
- **Inteligencia de tablero de instrumentos:** Ver destacados y estadísticas de gestión de destino actividades.
- **Entidad de Gestión:** Gestionar objetivos por grupos de interés (por ejemplo, medicamentos, terrorismo, delitos graves, ubicación, etc...)
- **Análisis de la Línea de Tiempo:** revisión y analizar los datos recogidos de una búsqueda avanzada determinado plazo
- **Búsqueda Avanzada:** de conducta de términos, nombres, palabras clave y números para recuperar información específica

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

*"Fecha de la clasificación	México, D.F. a 16 de octubre de 2014
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	Reservada
Partes o Secciones reservadas o confidenciales	Totalmente
Fundamento Legal	13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.
Ley específica	Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.
Periodo de reserva	Hasta 12 años" (sic)
Rúbrica del Titular de la Unidad Administrativa	

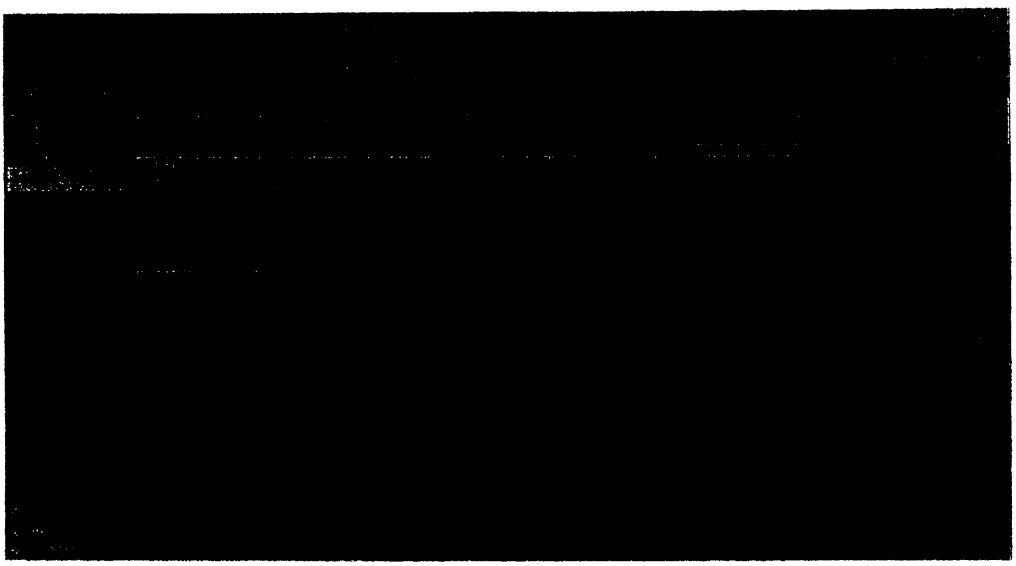
Los datos recogidos es organizados por grupos de interés (por ej., drogas, grupo A, grupo terrorista B, etc.) y cada grupo se compone de objetivos. Cada objetivo se compone de varios dispositivos que algunos agentes han instalados en ellos.

Los datos recogidos se muestran en una interfaz de usuario intuitivo fácil de utilizar y cuando corresponda emula popular visualización de aplicaciones comunes. La intuitiva interfaz de usuario está diseñada para un trabajo cotidiano. Los operadores pueden personalizar fácilmente el sistema ajuste sus métodos de trabajo preferido, definir reglas y alertas para temas específicos de interés.

El operador puede elegir ver los datos recogidos todo de blanco específico o sólo determinado tipo de información como información de ubicación, registro de calendario, correos electrónicos o mensajes instantáneos.

Calendario de Pegasus control pantalla se muestra en la figura 7.

Figura 7: Calendario de Monitoreo



PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Pantalla intercepción registro de llamadas Pegasus y la llamada se muestra en la Figura 8.

Figura 8: Registro de Llamadas y Llamada Intercepción

Pantalla de seguimiento Pegasus ubicación se muestra en la figura 9.

Figura 9: Ubicación de seguimiento

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, Incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

2: Presentación de los datos almacenados

Servicio / Tipo de Aplicación	Datos extraídos	Método de visualización
Mensajería Instantánea: 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	• Chat de participantes (Nombres y Teléfonos) • Contenido de conversación • Datos y Tiempo • Metadatos adjuntos (sin adjuntos)	• Cuadricula • Modo de conversación
Seguimiento de la ubicación	• Fuente de datos (GPS/CELL-ID) • Latitud • Longitud • Fecha y Hora	• Cuadricula • Mapa: - Visual en mapa - Ruta completa - Tipo de datos
Calendario	• Objetivo de reunión • Fecha de evento y tiempo de inicio	• Cuadricula • Vista mensual del calendario (emula calendario de clientes populares)
Detalles de contacto	• Valores totales guardados en el total de contactos incluyendo fotos si están disponibles.	• Cuadricula • Tarjeta de contacto con detalles completos
Sonido ambiental grabado (grabación de micrófono)	• Audio grabado • Fecha y hora grabada • Duración	• Cuadricula Interfaz de reproducción
SMS	• Dirección (entrante, saliente) • Nombre de contacto • Número de teléfono • Contenido de mensaje • Fecha y tiempo	• Cuadricula
Intercepción de llamada	• Dirección (entrante, saliente) • Nombre de contacto • Número de teléfono • Contenido de mensaje • Fecha y tiempo	• Cuadricula • Interfaz de reproducción
Email: 1. Aplicación de Email principal en todas las plataformas. 2. Aplicaciones Gmail en Android	• Desde • A • CC • BCC • Tema • Carpeta • Cuenta • Contenido de mensaje • Fecha y Hora	• Cuadricula • HTML (emula correo de clientes populares)

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Servicio / Tipo de Aplicación	Datos extraídos	Método de visualización
Recuperación de archivos	• Lista de carpeta (árbol) • Lista de archivos (cuadricula) • Nombre del archivo • Fecha modificada • Tamaño de archivo	• Cuadricula Vista de árbol
Toma de fotografía	• Fecha de modificación • Tamaño de archivo	• Cuadricula • Visualización de foto
Captura de pantalla	• Fecha y hora • Foto	• Cuadricula • Visualización de foto
Historial de búsqueda	• Fecha y hora • Imagen de captura de pantalla	• Listado
Favoritos de búsqueda	• Nombre de sitio web (salvado como el objetivo, usualmente el nombre del sitio web por default) • Dirección URL del sitio web	• Listado
Historial de llamadas (log de llamada)	• Dirección • Nombre de contacto • Número de teléfono • Duración • Fecha y hora	• Cuadricula
Información de dispositivo	• Nivel de batería • Tipo de conexión (ejemplo, 3G, WiFi) • MSISDN • IMEI • IMSI • Fabricante del dispositivo • Modelo de dispositivo • Versión de Sistema Operativo • Fecha de instalación • Tiempo de última conversación • País de origen del dispositivo • Servicio de red • Servicio de red en casa	• Panel de control

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 15 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Reglas y Alertas

El módulo de alertas de las reglas de las alertas del sistema al importante evento lleva a cabo. Las reglas deben definirse con antelación y ayudan a los operadores a revisar y tomar acciones en tiempo real, por ejemplo:

- **Geo-cercas:** o acceso zona caliente - alerta cuando objetivo llegar a una localización importante o licencia zona caliente - alerta cuando blanco dejó un lugar determinado alertas de Geo-cerca se basan en un perímetro alrededor de un lugar determinado, donde el operador define el tamaño del perímetro

- **Detección de conexión:**
  - Alerta Cuando se envía un mensaje desde / hasta el número específico
  - Alerta Cuando la llamada telefónica es protagonista desde / hasta el número específico.

- **Detección de contenido:** Alerta Cuando se utiliza la palabra / término / palabra definida en el mensaje codificado

Exportación de datos

El sistema está diseñado como un sistema end-to-end, proporcionando a sus usuarios con herramientas de recopilación y análisis. Sin embargo, entiende que existen requisitos de análisis avanzado datos y capacidades de fusión de otras fuentes, por lo tanto, el sistema permite la exportación de la información recopilada y una perfecta integración con back-end o el análisis de sistemas de terceros disponibles

Mantenimiento del Agente

Una vez que el agente está instalado en un determinado dispositivo, tiene que mantenerse con el fin de apoyar nuevas características y cambiar sus ajustes y configuraciones o a ser desinstalado cuando ya no está proporcionando inteligencia valiosa a la organización.

Actualización del Agente

Cuando se liberan las actualizaciones de los agentes que estén disponibles para instalar. Ahora están listos para la instalación en dispositivos nuevos objetivos o como actualizaciones existentes los agentes instalados en los dispositivos de destino estos nuevos agentes. Estas actualizaciones proporcionan nuevas funcionalidades, fallo de fijación, soporte para nuevos servicios o mejorar los agentes comportamiento global. Dichas actualizaciones son cruciales para mantener al agente funcional y operativa en el progreso sin fin del mundo de la comunicación y especialmente la arena Smartphone.

Existen dos tipos de actualizaciones de agente:

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

- Actualización opcional: no es obligatorio por el sistema. El usuario decide cuándo, si acaso, para actualizar el agente.
- Actualización obligatoria: de agente es obligatorio por el sistema. El supervisor debe actualizar al agente lo contrario que ninguna nueva información será monitoreada desde el dispositivo.

Actualización a veces requiere una instalación de un nuevo agente y a veces una pequeña actualización del agente existente. En ambos casos el usuario es el único para decidir cuándo realizar la actualización y por lo tanto debe planear esto por consiguiente.

Una vez que el comando de actualización fue enviado por el usuario, el proceso debería tomar sólo unos pocos minutos. El proceso podría tomar más tiempo si el dispositivo está apagado o tiene conexión de datos. En cualquier caso, la actualización se realizará una vez que disponga de una conexión de datos decente.

Configuraciones del Agente

Actualización a veces requiere una instalación de un nuevo agente y agente para ajustar por primera vez durante su instalación. Desde este punto, estos ajustes sirven al agente, pero siempre se pueden cambiar si es necesario. La configuración incluye la dirección IP para la transmisión de los datos recogidos, los comandos de forma son enviados al agente, el tiempo hasta que el agente se desinstala automáticamente sí mismo (véase el mecanismo de autodestrucción para más detalles) y mucho más.

Desinstalación del Agente.

Cuando se realiza la operación de inteligencia o en el caso donde el objetivo ya no es con interés a la organización, se puede quitar y desinstalar el componente de software base ("agente") en el centrador de. Desinstalar es rápido, requiere una solicitud de usuario único y no tiene ningún efecto al mínimo en el dispositivo de destino. Los temas de usuario una solicitud para el agente de desinstalación que se envía al dispositivo.

Una vez que el agente se desinstaló desde ciertos dispositivos no deja ningún rastro alguno o indicaciones fue alguna vez existieron 4.

Mientras el agente está en funcionamiento en el dispositivo y existe una conexión entre él y los servidores que puede ser fácilmente y de forma remota desinstalado.

Desinstalar siempre se puede hacer remotamente sin importar lo que fue el método utilizado para la instalación.

Desinstalar físico también es una opción, si es necesario.

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Desinstalar a un agente no significa perder los datos recogidos todo – los todos los datos que recogieron durante el tiempo que el agente fue instalado en el dispositivo se mantendrá en los servidores para futuros análisis.

Mecanismos de Autodestrucción

El sistema Pegasus Contiene mecanismos de autodestrucción para los agentes instalados. En general, Entender que si es más importante que el origen y los destinos no estarán expuestos a nada sospechoso de mantener el agente vivo y trabajo. Los mecanismos son en los Activados siguientes escenarios:

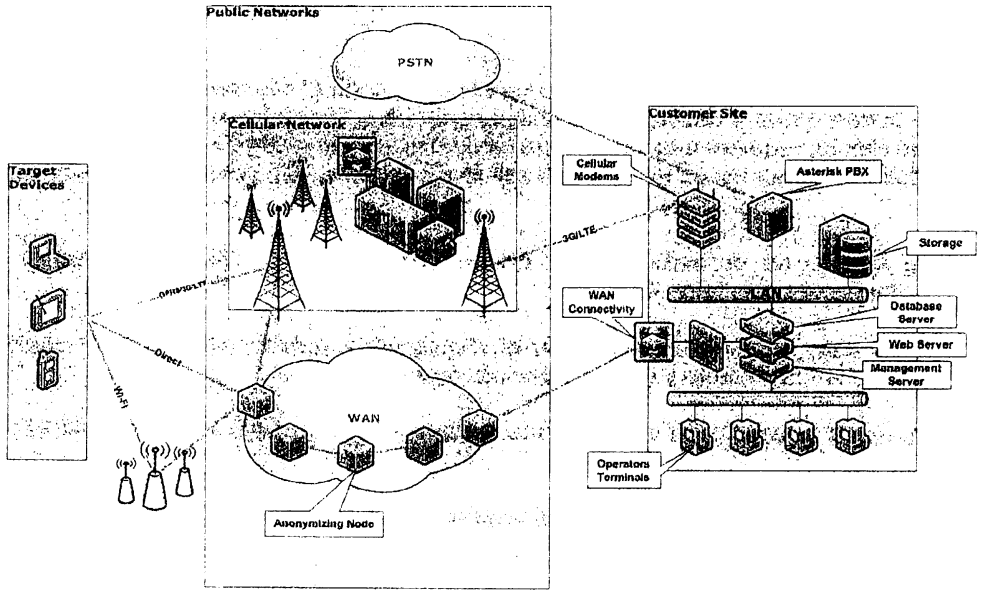
- **El riesgo de exposición:** en casos donde existe una gran probabilidad de que la exposición al agente, el mecanismos de autodestrucción se activa automáticamente y el agente se desinstala. Agente se puede instalar una vez más en un momento posterior.

- **Agente no responde:** en los casos en que el agente no responde y no lo hicieron comunique con los servidores durante mucho tiempo, El agente te desinstalar automáticamente. Estar expuesto a sí preventa o mal utilizados.

Solución de la Arquitectura

Principales componentes de la arquitectura del sistema Pegasus se muestran en la Figura 10.

Figura 10: Arquitectura de la solución



PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos a) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Sitio del Cliente.

NSO es responsable de implementar y configurar el hardware del Pegasus y software en las instalaciones del cliente, asegurándose de que el sistema está trabajando y funcionando correctamente. A continuación se presentan los principales componentes instalados en el sitio del cliente:

Servidor Web

Que residen en las instalaciones del cliente, los servidores son responsables de lo siguiente:

- Instalación del agente y mantenimiento
- Agente de monitoreo: controlar remotamente, configurar y actualizar agentes instalados
- Transmisión de datos: recibir la recogida datos transmitidos desde los agentes instalados
- Terminales de los operadores

Módulo de Comunicaciones

El módulo de comunicaciones permite la interconectividad y la conexión a internet a los servidores.

Módulo de comunicación celular

El módulo de comunicación celular permite la instalación remota del agente Pegasus al dispositivo de destino utilizando módems celulares o pasarelas SMS.

Módulo de permiso

El módulo de gestión de permisos Pegasus define y controla las características y
El contenido disponible permitido para cada usuario en función de su papel, el rango y jerarquía.

Almacenamiento de Datos

Los datos recogidos que se extrajo y vigilados por los agentes se almacenan en un dispositivo de almacenamiento externo. Los datos están bien respaldados y con resiliencia completo y redundancia para prevenir fallas y tiempo de inactividad.

Seguridad de Servidores

Todos los servidores residen dentro de la red del cliente confiable, detrás de las medidas de seguridad que puede implementar así como medidas de seguridad que suministramos específicamente para el sistema.

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Hardware

El hardware estándar del sistema está desplegado en varios servidores conectados juntos par de estantes. El equipo se encarga de balanceo de carga avanzada, compresión contenido, administración de conexión, cifrado, enrutamiento avanzado y altamente configurable servidor vigilancia del estado de monitoreo

Consolas de operador

Los terminales del operador punto final (PC) son la principal herramienta que los operadores de activar el sistema Pegasus, iniciar las instalaciones y los comandos y ver los datos recopilados

Aplicación Pegasus

La aplicación de Pegasus es la interfaz de usuario que está instalada en el terminal de operador. Proporcionan los operadores con la gama de herramientas para ver, ordenar, filtro, gestionar y alerta para analizar la gran cantidad de datos recogidos de los agentes de los objetivos

Redes Públicas

Aparte de ferretería e instalación del software en las instalaciones del cliente, el sistema Pegasus no requiere ninguna interfaz física con los operadores de red móvil local. Sin embargo, puesto que se transfieren los datos y las instalaciones del agente sobre las redes públicas, wemakes que se transfiere en la más eficiente y segura, todo el camino de vuelta a los servidores del cliente:

Redes de Anonimato

Pegasus anonimizar transmisión Network (red) está construido de anonimizar los nodos de conectividad que se distribuyen en diferentes lugares alrededor del mundo, permitiendo a agente conexiones ser dirigido a través de diferentes caminos antes de llegar a los servidores de Pegasus. Los nodos anónimos servir a sólo un cliente y se pueden configurar el cliente si es necesario.

Ver más información en la sección de transmisión red de anonimato de Pegasus.

Dispositivos de Destino

La arquitectura antes mencionada permite a los operadores a emitir las nuevas instalaciones, extraer, monitorear y activamente recopilar datos desde dispositivos de objetivos.

Nota: La Pegasus es un sistema de misión crítica de inteligencia, por lo tanto es completamente redundante para evitar averías y fallos. El sistema maneja grandes cantidades de datos y tráfico 24 horas al día y es escalable para apoyar el crecimiento del cliente y necesidades futuras

PGR
PROCURADURÍA GENERAL DE LA REPÚBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Solución de Hardware

Las especificaciones de hardware para el funcionamiento del sistema Pegasus depende del número de agentes instalados concurrentes, el número de estaciones de trabajo, la cantidad de datos almacenados y por cuánto tiempo deben guardarse.

Todo el hardware necesario es suministrado con el sistema al despliegue y requerir personalización local que tiene que ser manejado por el cliente en función de que las direcciones. Si es necesario, hardware puede adquirirse por el cliente en función de las especificaciones proporcionadas por nosotros.

Operadores de Terminales

Los operadores de las terminales son unidades estándar de escritorio, con las siguientes especificaciones:

- Procesador: Core i5
- Memoria: 3 GB de RAM
- Disco Duro: 320 GB
- Sistema operativo: Windows 7

Sistema de Hardware

Para apoyar plenamente la infraestructura del sistema, el siguiente hardware se requiere:

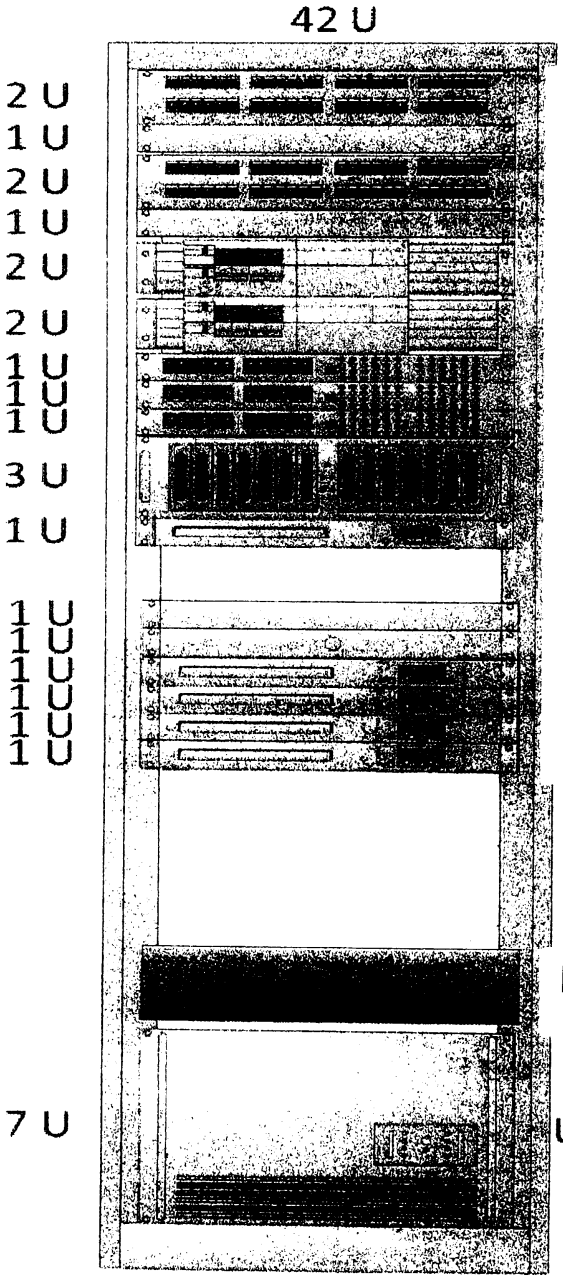
- Dos unidades de 42U gabinete
- redes hardware
- 10TB de almacenamiento
- 5 servidores estándar
- UPS
- celular módems y tarjetas SIM

El esquema de hardware del sistema se muestra en la figura 11.

PGR
PROCURADURIA GENERAL DE LA REPUBLICA

"Fecha de la clasificación	*México, D.F., a 16 de octubre de 2014*
Unidad Administrativa:	Centro Nacional de Planeación Análisis e Información para el Combate a la Delincuencia
Clasificación:	*Reservada*
Partes o Secciones reservadas o confidenciales	*Totalmente*
Fundamento Legal	*13 fracciones I, IV y V y 14 fracción I de la Ley de Federal de Transparencia y Acceso a la Información Pública Gubernamental. Lineamiento Décimo Octavo fracción II y V, incisos c) y d) y Vigésimo Cuarto fracción II de los Lineamientos Generales para la clasificación y desclasificación de la información de las dependencia y entidades de la Administración Pública Federal.*
Ley específica	*Artículo 40 Fracción XXI de la Ley que establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública.*
Periodo de reserva	*Hasta 12 años"* (sic)
Rúbrica del Titular de la Unidad Administrativa	

Figure 11: Pegasus Hardware



TRANSLATION[1]

TECHNICAL ANNEX

PURCHASE OF THE "PEGASUS" SYSTEM, IN ORDER FOR THE OFFICE OF THE ATTORNEY GENERAL OF THE REPUBLIC TO CONDUCT SUBSTANTIVE ACTIVITIES

DESCRIPTION OF "THE ASSET"

Description of **"THE ASSET"** is specified in the quotation issued by **"THE SUPPLIER,"** dated October 24, 2014, which is added to be part of this Memorandum of Understanding.

High-Level Architecture

The "Pegasus" system has been designed in layers. Each layer is responsible for jointly creating a comprehensive cyber intelligence collection and analysis solution.

The main layers and building blocks of the systems are:

- **Installations:** The Installation layer is in charge of issuing new agent installations, upgrading and uninstalling existing agents.

- **Data Collection:** The Data Collection layer is in charge of collecting the data from the installed device. "Pegasus" offers comprehensive and complete intelligence by using four collection methods:

- **Data Extraction:** Extraction of all existing data on the device upon agent installation.
- **Passive Monitoring:** Arrival of new data to the device.
- **Active Collection Monitoring:** Activate the camera, microphone, GPS and other elements to collect real-time data
- **Event-based Collection:** Define scenarios which automatically trigger specific data collection
- **Data Transmission:** The data transmission layer is in charge of transmitting the data back to the command and control servers, using the most efficient and safe way
- **Presentation Analysis:** The presentation/analysis component is a user interface in charge of presenting the collected data to the operators and analysts, turning the data into intelligence data. This is done by using the following modules:

[1] Translator's Note: All pages of the original document (pp. 17-54) bear two initials at the bottom of each page.
Also, there is an insert on the top right-hand side of each page which has been listed following p. 54 and applies to all pages, as the original font is small and hard to read.
Reference to footnotes is made in the text, but no footnote description is given.
This document seems to have been translated from the English by non-professional translators. At times, Spanish words are put together in sequence that do not make any sense, or a word is used within a sentence that does not make sense, either. This has been noted by this translator by placing a question mark between brackets.
English words appear sometimes in the middle of a sentence that also do not make sense; this has been noted with a [*sic*] notation next to the word.

- **Real-Time Monitoring:** Presents real-time collected data from specific or multiple targets. This module is very important when dealing with sensitive targets or during operational activities, where each piece of incoming information is crucial for decision-making.

- **Offline Analysis:** Advanced queries mechanism allowing the analysts to query and retrieve any piece of collected information. The advanced mechanism provides tools to find hidden information and connections.

- **Geo-based Analysis:** The data collected data are presented on a map and geo-based queries conducted.

- **Administration:** The administration component is in charge of managing permission for the entire system permission, security and health: extracted messages contacts, e-mails, photographs, files, locations, passwords, list of process and more.

- **Permission:** The permissions mechanism allows the system administrator to manage the system's various users. It provides each one of them the right access level only to the data they are allowed to access. This allows to define groups within the organization which handle only one or more topics and other groups which handle different topics.

- **Security:** The security module monitors the system's security level, making sure the collected data is entered into the system's database clean and safe for future review.

- **Health:** The health component of the "Pegasus" solution monitors the status of all components, making sure everything is working smoothly. It monitors the communication among the various parts, the system's performance, the storage availability and alerts if anything malfunctions.

Hardware Solution

The hardware specifications for operating the Pegasus system depend on the number of concurrently installed agents, the number of working stations, the amount of stored data and how long they should be stored.

All necessary hardware is supplied with the system upon deployment, and it requires local customization to be managed by the customer based on the instructions. If required, hardware can be purchased by the customer, based on the specifications provided by us.

Terminal Operators

Terminal operators are standard desktop PCs, with the following specifications:

- Processor: Core i5
- Memory: 3 GB RAM

- Hard disc: 320 GB
- Operating system: Windows 7

System's Hardware

To fully support the system's infrastructure, the following hardware is required:

- Two 42U desk units
- Hardware networks
- 10TB of storage
- 5 standard servers
- UPS
- Cellular modems and SIM cards

WARRANTY, MAINTENANCE AND UPGRADES OF "THE ASSET"

"THE ASSET'S" warranty shall be 12 months from the date of receipt thereof. **"THE SUPPLIER"** undertakes to provide maintenance to **"THE ASSET"** and to provide support, free of charge, to the **"ATTORNEY GENERAL'S OFFICE,"** pursuant to the following:

Maintenance and Support

"THE SUPPLIER" shall provide maintenance and three-tier support services, including:

- **Tier 1:** Standard-system operational issues involving email and telephone support
- **Tier 2:** Proactive resolution of technical issues with dedicated engineers who will inspect, examine and resolve common technical issues, by using their best efforts and providing remote assistance by using remote desktop software and a virtual private network (VPN) when so requested
- **Tier 3:** Fixing system failures and system updates of significant system malfunctions

Telephone Support: In addition to the above, **"THE SUPPLIER"** shall provide a telephone number and email address for any questions and to resolve any issues.

In addition, "THE SUPPLIER" shall be able to provide the following additional support:

- Planned or emergency on-site assistance
- Health monitoring system

[LOGO] PGR – PROCURADURÍA GENERAL DE LA REPÚBLICA
(OFFICE OF THE ATTORNEY GENERAL OF THE REPUBLIC)

QUOTATION ISSUED BY "THE SUPPLIER," DATED OCTOBER 24, 2014

Introduction

Pegasus is a world-leading cyber intelligence solution enabling law-enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device.]This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battle. By capturing new types of information from mobile devices, Pegasus is [*sic*] a substantial technology gap offering the most complete and accurate intelligence for your security operations.

Smartphone Interception Challenge

The highly dynamic and growing mobile communications market – characterized by the introduction of new devices, operating systems and applications virtually on a daily basis – requires a rethinking of the traditional intelligence paradigm. These changes in the communications landscape pose real challenges and obstacles that must be overcome by intelligence organizations and law-enforcement agencies worldwide:

- Encryption: Extensive use of encrypted devices and applications to convey messages
- Abundance of communication applications: Chaotic market of sophisticated applications, most of which are IP-based and use proprietary protocols
- Target outside interception domain: Targets' communications are often outside the organization's interception domain or otherwise inaccessible (e.g., targets are roaming, face-to-face meetings, use of private networks, etc.)
- Masking: Use of various virtual identities which are nearly impossible to replace by SIM card
- Monitoring and tracking: SIM card replacement to avoid any kind of data extraction
- Frequent Interception: Most of the information is not sent over the network or shared with other parties and is only available to the end-user device
- Complex and costly implementation: As communications become increasingly complex, more network interfaces are required. Setting up these interfaces with service providers is a lengthy and costly process, which requires regulation and standardization

Standard Interception Solutions are not Enough

Until the above-mentioned challenges are addressed and objectives resolved, criminals and terrorists are likely "safe" from standard systems and legacy interception, meaning that valuable intelligence is being lost. These standard solutions (described in the sections below) deliver only partial intelligence, leaving the organizations with substantial intelligence gaps.

Passive Interception

Passive interception requires very deep and close relationships with local service providers (cellular, Internet and PSTN providers) and, traditionally, it has allowed for proper monitoring of text messages and voice calls. However, most contemporary communications consist of IP-based traffic, which is extremely difficult to monitor with passive interception due to its use of encryption and proprietary protocols.

Even when this traffic is intercepted, it typically carries massive amounts of technical data that are not related to the actual content and metadata being communicated. Not only does this result in frustrated analysts and wasted time wading through irrelevant data, it also provides a partial snapshot (the best one) of the target's communications. In addition, the number of interfaces required to cover the relevant service providers broadens the circle of entities exposed to sensitive information and increases the chance of leakage.

GSM Tactical Interception

GSM tactical interception solutions effectively monitor voice calls and text messages in GSM networks. When advanced cellular technologies are deployed (3G and LTE networks), these solutions become less efficient. In such cases, it is required to violently downgrade the target from a GSM-based network, which significantly impacts the user’s experience and functionality.

These solutions also require a well-trained tactical team and an area located near the monitored target. Thus, in the majority of cases where the target location is unknown, these solutions become irrelevant. In other cases, placing a tactical team close to the target may pose serious risks both to the team and the entire intelligence operation.

Malware

Malware presumably provides access to the target's mobile device. However, it is not completely transparent and requires the target's involvement to be installed on his devices. This type of engagement usually takes on the form of multiple confirmations and approvals before the malware becomes functional. Most targets are unlikely to be fooled into cooperating with malware due to their high level of sensitivity for privacy in their communications.

In addition, such malware is likely to be vulnerable to most commercially available anti-spyware and anti-virus software. As such, they leave traces and are fairly easily detected on the device.

Cyber Intelligence for the Mobile World

Pegasus is a world-leading cyber intelligence solution enabling law-enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device. This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battle.

By capturing new types of information from mobile devices, Pegasus bridges a substantial technology gap to offer the most complete and accurate intelligence for your security operations. This solution is able to penetrate the market's most popular smartphones based on BlackBerry, Android, iOS and Symbian operating systems.

Pegasus silently deploys invisible software ("agent") on the target device. This agent then extracts and properly transmits the collected data for their analysis. Installation is performed remotely (OTA) and does not require any action from or engagement with the target, leaving no trace whatsoever on the device.

Pegasus Benefits

Organizations which deploy Pegasus are able to overcome the above-mentioned challenges to achieve unmatched mobile intelligence collection:

Unlimited access to target's mobile devices: Remote and covert collection of information about your target's relationships, location, phone calls, plans and activities - whenever and wherever they are.

Intercept calls: Transparent monitoring of voice and VoIP calls on real-time intelligence gaps.

- Bridging: Collection of unique and new types of information (e.g., contacts, files, environmental monitoring, passwords, etc.) to deliver the most accurate and complete intelligence.

- Handling encrypted content and devices: Overcome encryption, SSL, proprietary protocols and any obstacles posed by the complex monitoring of applications [and] global communications.

- Monitoring a multitude of applications, including targets, such as: Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)

- Target monitoring: Securing information by using independent GPS

- Precise positioning service provider: No cooperation with local mobile network operators (MNO) is required

- Discovery of virtual identities: Constant monitoring of the device without worrying about frequent switching of virtual identities and replacement of SIM cards

- Avoidance of unnecessary risks: Eliminate the need for physical proximity to the target or device at any stage

Technology Highlights

The Pegasus solution utilizes cutting-edge technology specially developed by veterans of intelligence and law-enforcement agencies. It offers a rich set of advanced features and sophisticated intelligence collection capabilities not available in standard interception solutions:

- Penetration of Android, BlackBerry, iOS and Symbian-based devices
- Access to password-protected devices
- Totally transparent to the target
- No trace left on the device
- Minimal battery, memory and data consumption
- Self-destruction mechanism in case of exposure/risk
- Retrieval of any file from the device for deeper analysis

High-Level Architecture

The Pegasus system is designed in layers. Each layer is responsible for jointly creating a comprehensive cyber intelligence collection and analysis solution.

The systems' main layers and building blocks are:

- Installations: The installation layer is in charge of issuing new agent installations, upgrading and uninstalling existing agents.
- Data Collection: The data collection layer is in charge of collecting the data from the installed device. Pegasus offers comprehensive and complete intelligence by using four collection [methods]:
  - Data Extraction: Extraction of all existing data on the device upon agent installation
  - Passive Monitoring: Monitoring new incoming data to the device
  - Active Monitoring/Collection: Activate the camera, microphone, GPS and other elements to collect real-time data
  - Event-based Collection: Definition of scenarios that automatically trigger specific data collection
- Data Transmission: The data transmission layer is in charge of transmitting the data to the command and control servers, by using the most efficient and safe way
- Presentation Analysis: The presentation/analysis component is a user interface in charge of presenting the collected data to operators and analysts, turning the data into intelligence. This is done by using the following modules
- Real-Time Monitoring: Presentation of real-time collected data from specific or several targets. This module is very important when dealing with sensitive targets or during operational activities, where each incoming piece of information is crucial for decision-making.
- Offline Analysis: Advanced queries mechanism allowing analysts to query and retrieve any piece of collected information. The advanced mechanism provides tools to find hidden information and connections.
- Geo-based Analysis: Presentation of collected data on a map and performance of geo-based queries.
- Administration: The administration component is in charge of managing the entire system's permission, security and health: contacts of extraction [*sic*][,] messages, emails, photos, files, locations, passwords, processes list, etc.
- Permission: The permission mechanism allows the system's administrator to manage the various system's users, providing each of them the right access level only to the data they are allowed to. This allows the definition of groups within the organization that handle just one or more topics and other groups that handle different topics.
- Security: The security module monitors the system's security level, making sure the collected data is entered into the system's database clean and safe for their future review.
- Health: The health component of the Pegasus solution monitors the status of all components, making sure everything is working smoothly. It monitors communication among the various parts, the system's performance, information storage availability and warns if anything malfunctions.

The system's ayers and components are shown in figure 1.

Figure 1: Pegasus high-level architecture

[INSERT FIGURE ON P. 29]

Agent Installation

In order to start collecting data from your target's smartphone, a software-based component ("agent") must be remotely and covertly installed on their device.

Agent's Purpose

The "agent," a software-based component, resides on the end-point devices of the monitored targets, its purpose being to collect the data for which it was configured. The agent is compatible with the most popular operating systems: BlackBerry, Android, iOS (iPhone) and Symbian-based devices.

Each agent is independent and is configured to collect different information from the device, and to transmit the signal via specific channels in defined timeframes. The data are sent back to the Pegasus servers in a concealed, compressed and encrypted manner.

The agent continuously collects information from the device and will transmit it once reliable Internet connection becomes available.

Communications encryption, the use of many applications and other communications-concealing methods are no longer relevant when an agent is installed on the device.

Agent Installation Vector

Injectables and installing an agent on the device are the most sensitive and important stages of the intelligence operation performed on the target's device. Each installation must be carefully planned to ensure its success. The Pegasus system supports various installation methods. The variety of installation methods corresponds to the different operational scenarios which are unique to each customer, resulting in the most comprehensive and flexible solution. Following are the accepted installation vectors:

Remote Installation (Range):

- Over-the-Air (OTA): A push message is remotely and covertly sent to the mobile device. This message triggers the device to download and install the agent on the device. Throughout the installation process target's cooperation or engagement is required (e.g., clicking a link, opening a message) and no indication appears on the device. Installation is totally silent and invisible and cannot be prevented by the target. This is the uniqueness of NSO, which significantly differentiates the Pegasus solution from any other solution available on the market.

- **Enhanced Social Engineering Message (ESEM):** In cases where the OTA installation method cannot be applied[1], the system's operator can choose to send a regular text message (SMS) or an email, luring the target to open it. Single click, either planned or unintentional, on the link will result in concealed agent installation. The installation is totally concealed, and although the target clicked the link, he will not be aware that software is being installed on his device.

The chances that the target will click the link are totally dependent on the level of content/ credibility. The Pegasus solution provides a wide range of tools to compose an innocent message, tailored to lure the target to open the message.

Note: Both OTA and ESEM methods only require a telephone number or an email address used by the target. Nothing else is required to accomplish a successful installation of the Pegasus agent on the device.

Close to the Target (Limited Range):

- **Tactical Network Element:** The Pegasus agent can be silently injected once the number is obtained by means of the tactical network element, such as **Base Transceiver Station** (BTS). The Pegasus solution leverages the capabilities of these tactical tools to perform a remote injection and installation of the agent. In most cases, taking a position in the target's area is sufficient to obtain the phone number. Once the number is available, the installation is remotely performed.

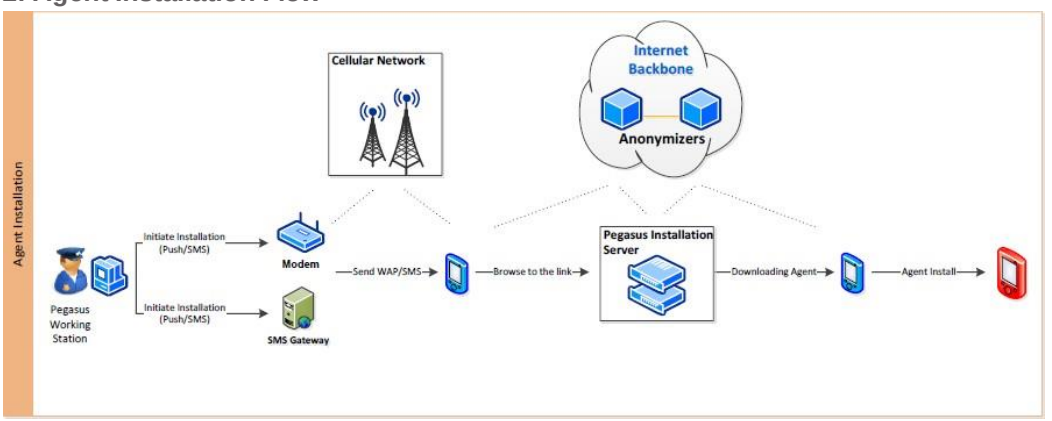
- **Physical:** When physical access to the device is an option, the Pegasus agent can be manually injected and installed in less than five minutes. After agent installation, data extraction and future data monitoring are performed remotely, providing the same features as any other installation method.

Note: Tactical and physical installations are usually performed where no target telephone number or email address are available.

Agent Installation Flow

Remote agent installation flow is shown in Figure 2.

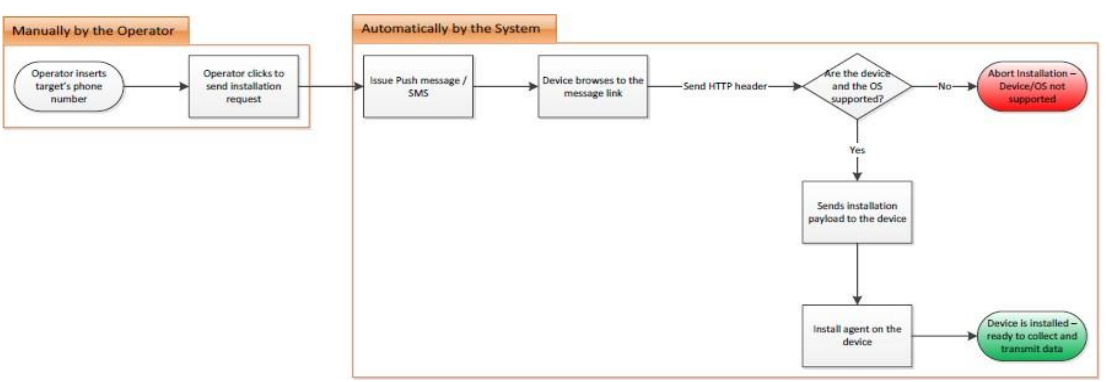
Figure 2: Agent Installation Flow



In order to initiate a new installation, the Pegasus system's operator only has to enter the target's phone number. The rest is automatically done by the system, resulting in most cases in an installed agent on the target's device.

Beginning of Agent set-up is shown in Figure 3.

Figure 3: Beginning Agent installation



Compatible Operating Systems & Devices

Operating System (OS)	OS Version	Device	Comments
Android	2.1 – 4.2	▪ Samsung Galaxy series ▪ Sony Ericsson Xperia series ▪ Others (refer to note below)	Support is based on local firmware versions, which must be defined with the customer
iOS	4.x – 6.1.4	▪ iPhone 4 ▪ iPhone 4S ▪ iPhone 5	
BlackBerry	5.0 – 7.1	▪ Curve (8520, 9300, 9350, 9360) ▪ Bold (9000, 9700, 9780, 9790, 9900, 9930) ▪ Torch (9800, 9810, 9850, 9860) ▪ Pearl (9100)	
Symbian	Version S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variety of devices	Support is based on local firmware versions, which must be defined with the customer

NOTE: Android-based devices are often added to the supported list. An updated list can be sent at the customer´s request.

Installation Failure

The installation can sometimes fail due to following reasons:

1. **Unsupported device:** the target device is not supported by the system (as listed above).

2. **Unsupported OS**: the operating system of the target device is not supported by the system.

3. **Unsupported Browser:** the device default browser was previously replaced by the target. Installation of browsers other than the device default (and also Chrome for Android-based devices) is not supported by the system.

In any of the above-mentioned cases, if the operator initiates a remote installation to a non-supported device, operating system or browser, the injection will fail and the installation will be aborted. In these cases, the process is finished with an open browser on the target device pointing and showing the URL page, which was defined by the operator prior to the installation. The device, OS and browser are identified by the system using their HTTP user agent. If, for any reason, the user's agent was manipulated by the target, the system might fail to correctly identify the device and OS and provide the wrong installation payload. In such case, the injection will fail and the installation will be aborted, showing again the above-mentioned URL page.

Data Collection

Upon successful agent installation, a wide range of data is monitored and collected from the device:

- **Textual:** Textual information includes text messages (SMS), emails, calendar records, call history, instant messaging, contact list, browsing history and more. Textual information is usually structured and small in size; therefore, easier to transmit and analyze.
- **Audio**: Audio information includes intercepted calls, environmental sounds (microphone recording) and other recorded audio files.
- **Visual:** Visual information includes camera snapshots, photo retrieval and screen captures.
- **Files:** Each mobile device contains hundreds of files, some of which contain invaluable intelligence, such as databases, documents, videos and more.
- **Location:** Continuous monitoring of device location (Cell-ID and GPS).

:

The variety of data collected by the Pegasus system is shown in Figure 4.

Figure 4: Collected Data

Data collection is divided into three levels:

- Initial extraction
- Passive monitoring
- Active data collection

Initial Data Extraction

Once the agent is successfully injected and installed on the device, the following data residing and existing on the device can be extracted and sent to the command and control center:

- SMS records
- Contact details
- Call history (log)
- Calendar records
- Email messages
- Instant messaging
- Browsing history

Unlike other intelligence collection solutions providing just future monitoring of partial communications, Pegasus allows the extraction of all existing data on the device. As a result, the organization benefits from accessing historical data about the target, which assists in building a comprehensive and accurate intelligence picture.

Note: Initial data extraction is an option and not a must. If the organization is not allowed to access the target's historical data, such option can be disabled and only new incoming data will be monitored by the agent.

Passive Monitoring

From the point the agent was successfully installed, it keeps monitoring the device and retrieves any new record that becomes available in real-time (or under specific conditions, if configured differently). The full list of data monitored by the agent appears below:

- SMS records
- Contact details
- Call history (log)
- Calendar records
- Email messages
- Instant messaging
- Browsing history
- Location tracking (Cell-ID based)

Active Collection

In addition to passive monitoring, upon successful agent installation a wide set of collection becomes available. Active collection refers to activating requests sent by operators to collect specific information from the installed *unscrew* [*sic*]. This set of features is called active, as collection thereof is at the implicit request of the operator. Active collection allows the operator to perform real-time actions on the target's device to retrieve unique information from the device and from the target's surrounding area, including:

- Location tracking (GPS-based)
- Voice calls interception
- File retrieval
- Environmental sound recording (microphone recording)
- Photo monitoring
- Screen capture

Active collection differentiates Pegasus from any other intelligence collection solution, as the operator controls the collected information. Instead of just waiting for information to come in, hoping this is the information he was seeking, the operator actively retrieves important information from the device, getting the exact information sought by him.

Description of Collected Data

The various types of data available for extraction, passive monitoring and active collection, with their respective features, are listed in Table 1.

Table 1: Description of Collection Features

Application Type	Description of Features	Data Extraction	Passive/Active Collection
Instant Messaging: 1. Whatsapp 2. Viber 3. Skype 4. Blackberry Messenger (BBM)	Agent extracts and monitors all incoming and outgoing instant messages to/from the device. One-on-one conversation extraction and monitoring, including group chat. Indication for file transfer (file name).	√	√
Location Tracking	The system provides two types of location information about the device: <u>GPS:</u> 1. At user's request, a defined timeframe for the sampling area is opened. GPS data are retrieved, when applicable (available reception). In case non-recovery is available, Cell-ID from GPS signal [?]. 2. If GPS is disabled by target, the system allows sampling to stop and turn off immediately occurs. <u>Cell-ID</u>: Devices constantly transmit their location (Cell-ID) each time they communicate with server. The retrieved location data are analyzed at the server and placed on the map. Location-based queries and alerts are easily fixed.	√	√
Calendar	Agent extracts all calendar records from the device and monitors any change or new event added to the calendar.	√	√
Contact Details	Agent extracts all contacts available on the device. Thus, the agent monitors any change/deletion of existing contacts and the addition of new ones. Agent extracts and monitors all values assigned to each available contact field (based on vCard fields), including the photo, if assigned.	√	√

Application Type	Description of Features	Data Extraction	Passive/Active Collection
Environmental sound recording (microphone recording)	User can request to turn on the device's microphone and listen to the surrounding sounds in real-time. The surrounding sounds are recorded and can be analyzed and replayed at a later stage. Turning on the microphone is based on a silent call from the server (PBX). Such call will be allowed only after the security agent is assured the device is in idle mode (device is not in active use and the screen is turned off). No action [*sic*] by the target that turns on the screen will result in immediate call hang-up and cease of capturing surrounding sounds. No indication of the recording or the incoming silent call appears on the device at any point. The quality of the recording depends on the sensitivity of the device's microphone, the surrounding noise and the device model. This sensitivity varies among the various mobile phone models and is set by the phone manufacturer. Usually, the content of a conversation held a few meters from the device can be heard.	N/A	√
SMS	Agent extracts and monitors all incoming and outgoing text messages (SMS).	√	√
Call Interception (call recording) – Only Android	User can request to record all incoming and outgoing calls from the target's device. Calls are locally recorded on the device and then sent to the server upon completion.	N/A	√
Email: 1. Email application on all platforms. 2. Gmail apps on Android	Agent extracts and monitors all emails found on the device. The main email app (action) is monitored; thus, all defined accounts are not monitored (i.e., exchange, Gmail, etc.). For Android-based devices, both the main email app and the Gmail app are monitored.	√	√
File Retrieval	Upon user's request, a full list of files and folders is extracted from the device (internal storage and SD card). When the operator comes across a file of interest, he can immediately request to retrieve it.	N/A	√

Picture taking	To the instant petition user using the front and rear camera from the device and sent to the servers [?]. Pictures are taken after security agent that the device is in idle mode [?]. During the picture having the indication it appears on the device and the flash is never used [?]. Picture quality can be chosen by the operator to reduce data usage and for fast photo transmission. Since flash is not used and telephone could be in motion or interior rooms might have low light, the pictures are sometimes out of focus.	N/A	√
Screen Capture	Upon user's request a screen capture is taken and sent to the Pegasus servers. Screen captures from the devices can provide information about the apps used by the target, background image used and the target's most private information.	N/A	√
Browsing History	Agent extracts and monitors browsed websites on the device default browser.	√	√
Browsing Favorites	Agents extract and monitor favorite websites saved on the device default browser.	√	√
Call History	Agent extracts the history of all incoming/outgoing calls made to/from the device. The data include the individual who placed the call, the numbers called and duration of the call. Call attempts which did not result in a conversation will show a duration of 0 (zero) seconds.	√	√
Call History	Agent extracts the history of all incoming/outgoing calls made to/from the device. The data include the individual who placed the call, the numbers called and duration of the call. Call attempts which did not result in a conversation will show a duration of 0 (zero) seconds.	√	√

The above-mentioned data are the potential data that can be collected by an agent. The agent will collect the data available the device and applicable. If one or more of the above-mentioned applications does not exist or has been removed from the device, the agent will operate in the same manner. The data will be collected from the rest of the services and applications which are in use on the device. Furthermore, all collected data from the removed application will be saved on the servers or at the agent, if not yet transmitted to the servers.

In addition, the above-mentioned data collected by the agent cover the most popular applications used worldwide. Since application popularity varies from country to country, we understand that data extraction and monitoring of other applications will be required as time evolves and new applications are adopted by targets. When such requirement arises, we can easily extract important data from virtually any application based on customer demand and launch it as a new release that will become available to the customer.

Collection Buffer

The installed agent monitors the data from the device and transmits it to the servers. If transmission is not possible3, the agent will collect the new available information and transmit it when connection becomes available. The collected data are stored in a hidden, encrypted buffer. This buffer is set to take up no more than 5% of the free space available on the device. For example, if the monitored device has 1GB of free space, the buffer can store up to 50MB. In case the buffer has reached its limit, the oldest data are deleted and new data are stored (FIFO). Once the data have been transmitted, the buffer content is totally deleted.

Data Transmission

By default, the collected data (initial data extraction, passive monitoring and active collection) are sent back in real-time to the command and control center. The data are sent via data channels, Wi-Fi being the preferred connection to be used, when available. In other cases, data transmission takes place via cellular data channels (GPRS, 3G and LTE). Extra thought has been given to compression methods and focusing on textual content transmission whenever possible. The data footprints are very small and usually take up only few hundred bytes. This is to make sure the collected data are easily transmitted, ensuring minimal impact on the device and on the target’s cellular data plan.

If data channels are not available, the agent will collect the information from the device and store it in a dedicated buffer, as explained in the Data Collection section.

Data transmission automatically stops under the following scenarios:

- **Low battery:** When the device battery level is below the defined threshold (5%), all data transmission processes immediately stop until the device is recharged.

- **Roaming device:** When the device is roaming, cellular data channels become pricey, thus data transmission is done only via Wi-Fi. If no Wi-Fi connection exists, transmission will stop.

When no data channels are available, and no indication for communication is coming back from the device, the user can request to communicate with the device or send some crucial data using text messages (SMS).

WARNING: Communication and/or data transmission via SMS may incur charges by the target and appear in his billing report; thus, this should be used sparingly.

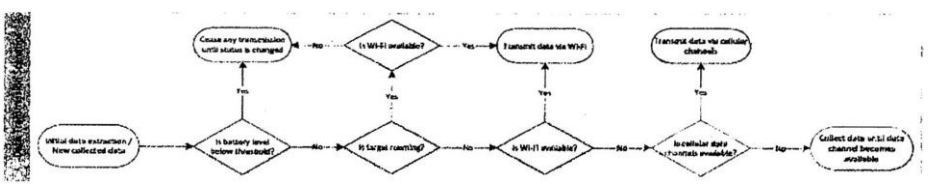
Communication between the agent and the central servers is indirect (through anonymizing network), so trace back to the origin is non-feasible.

The data transmission process of the Pegasus system is shown in Figure 5.

Figure 5: Data Transmission Process

Channels and scenarios for the transmission of collected data are shown in figure 6.

Figure 6: Data transmission scenarios



Data Transmission Security

All connections between the agents and servers are encrypted with strong algorithms and are mutually authenticated. While data encryption is probably the most pressing issue, additional care has been taken to ensure minimal data, battery and memory are consumed within the agents' requirements. This is meant to make sure that no concerns are raised by the target. Detecting an operating agent by the target is almost impossible. The Pegasus agent is installed at the kernel level of the device, it is well concealed and impossible to be found by antivirus and anti-spy software.

Transmitted data are encrypted with symmetric encryption AES 128-bit.

Pegasus Anonymyzing Transmission Network

Agent transparency and source security are the guiding principles of the Pegasus solution. To ensure that trace back to the operating organization is impossible, the Pegasus Anonymizing Transmission Network (Network), a network of anonymizers is deployed to serve each customer. The network nodes are spread in different locations around the world, allowing agent connections 6er [*sic*] to be redirected through different pathways prior to reaching the Pegasus servers. This ensures that the identities of both communicating parties are highly obscured.

Data Presentation and Analysis

Successful data collection from hundreds of targets and devices generates huge amounts of data for analysis, presentation and visualization. The system provides a set of operational tools to help the organization transform intelligence data to view, sort, filter, query and analyze the collected data. The tools include:

- Geographical analysis: Tracking target's real-time and historical location, several targets on the map
- Rules and alerts: Definition of rules to generate alerts upon arrival of important data
- Favorites: Marking important and favorite events for subsequent review and deeper analysis
- Instrument panel intelligence: Viewing highlights and statistics of target's activities
- Entity management: Management of targets by interest groups (e.g., drugs, terrorism, serious crime, location, etc.)
- Timeline analysis: Review and analysis of collected data from advanced search at a particular time frame
- Advanced search: Search for terms, names, key words and numbers to retrieve specific information

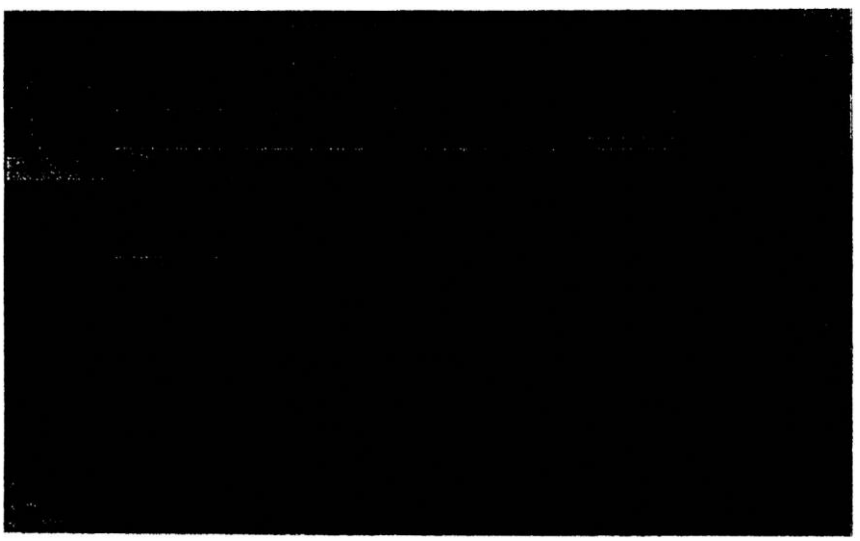
Collected data are organized by groups of interest (e.g., drugs, group A, terrorist group B, etc.), and each group consists of targets. Each target consists of several devices having some agents installed on them.

Collected data are displayed in an easy-to-use intuitive user interface and, when applicable, they emulate popular display of common applications. The intuitive user interface is designed for day-to-day work. Operators can easily customize the system to fit their preferred working methods, to define rules and alerts for specific topics of interest.

The operator can choose to view the entire collected data from specific target or only specific type of information, such as location information, calendar record, emails or instant messages.

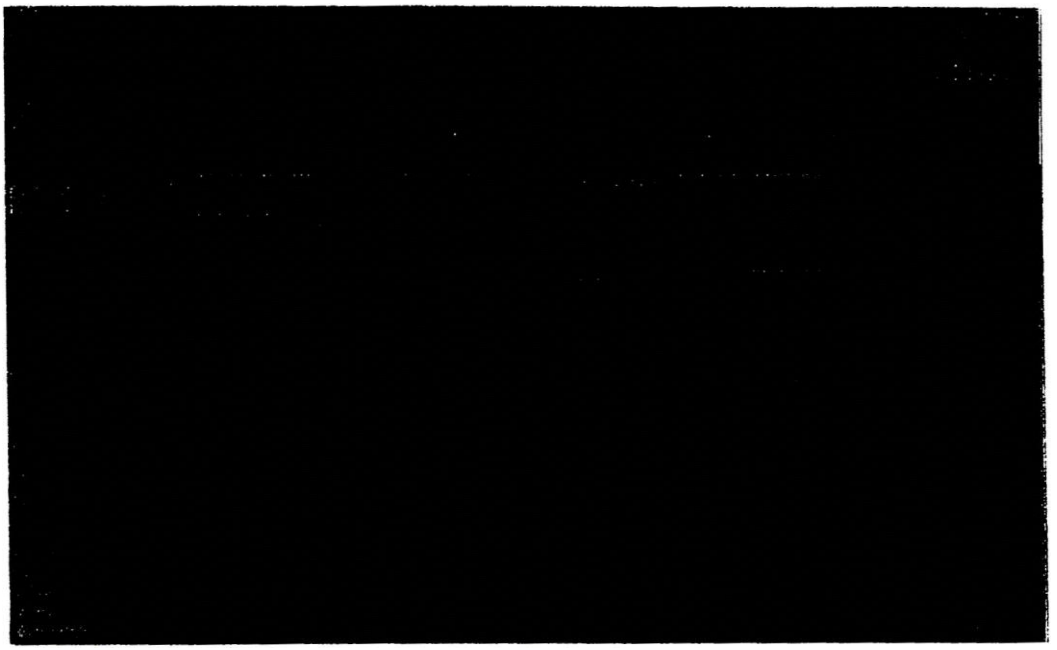
Pegasus calendar monitoring screen is shown in Figure 7.

Figure 7: Monitoring Schedule



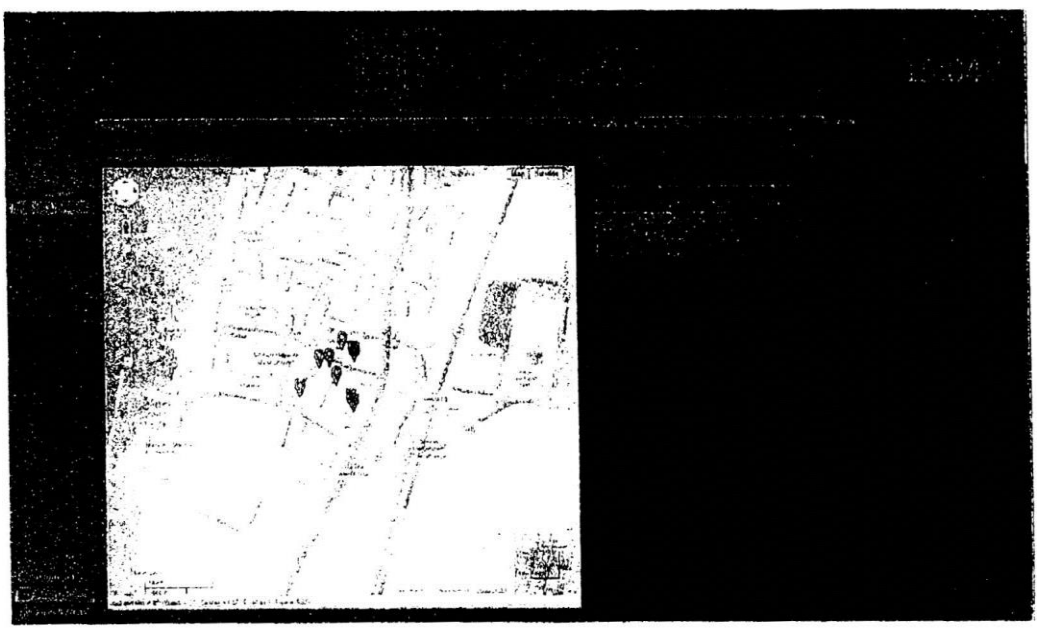
Pegasus call log interception screen and call are shown in Figure 8.

Figure 8: Call Log and Call Interception



Pegasus location tracking screen is shown in figure 9.

Figure 9: Location tracking



- **2: Presentation of Stored Data**

Service/Type of Application	Extracted Data	Display Method
Instant Messaging: 1. WhatsApp 2. Viber 3. Skype 4. Blackberry Messenger (BBM)	• Chat participants (names & phones) • Conversation content • Date and time • Metadata attachments (without attachments)	• Grid • Conversation mode
Location tracking	• Data source (GPS/Cell-ID) • Latitude • Longitude • Date and time	• Grid • Map - Map display - Full trail - Type of data
Calendar	• Meeting subject • Event date and start time	• Grid • Monthly calendar view (emulates popular calendar clients)
Contact details	• Total values stored in total contact entry, including photo, if available	• Grid • Contact card with full details
Environmental sound recording (microphone recording)	• Recorded audio • Recorded date and time • Duration	• Grid Playback interface
SMS	• Direction (incoming, outgoing) • Contact number • Telephone number • Message content • Date and time	• Grid
Call interception	• Direction (incoming, outgoing) • Contact name • Telephone number • Message content • Date and time	• Grid • Playback interface
Email 1. Main Email app on all platforms 2. Gmail apps on Android	• From • A • CC • BCC • Subject • Folder • Account • Message content • Date and time	• Grid • HTML (emulates popular email clients)

Service/Type of Application	Extracted Data	Display Method
File retrieval	• List of folders (tree) • List of files (grid) • Filename • Date modified • File size	• Grid • Tree view
Photo taking	• Date and time • Photo	• Grid • Photo viewer
Screen capture	• Date and time • Photo	• Grid • Photo viewer
Browing history	• Date and time • Screen capture image	• List
Browing favorites	• Website name (saved as the target, usually the default website name) • Website URL address	• List
Call history (call log)	• Address • Contact name • Telephone number • Duration • Date and time	• Grid
Device information	• Battery level • Connection type (i.e., 3G, WiFi) • MSISDN • IMEI • IMSI • Device manufacturer • Device model • Operating system version • Installation date • Last communication time • Device country of origin • Network service • Home network service	• Control panel

Rules and Alerts

The system's rules and alerts module alerts when an important event takes place. Rules must be defined in advance, and they help the operators to review and take real-time actions, for instance:

- Geo-fencing**:** or hot zone alert – alert when target arrives at an important location or hot zone license [?] -- alert when target left a certain location Geo-fence alerts are based on a perimeter around a certain location, where the size of the perimeter is defined by the operator.
- Connection detection:
  - Alert when a message is sent from/to a specific number
  - Alert when the phone call is made from/to a specific number
- Content detection:
  - Alert when a defined word/term/ word in coded message is used

Data Export

The system is designed as an end-to-end system, providing its users with collection and analysis tools. However, it is understood there are advanced data analysis requirements and fusion capabilities from other sources; therefore, the system allows exporting the collected information and seamless back-end integration or analysis with third-party available systems.

Agent Maintenance

Once the agent is installed on a certain device, it has to be maintained in order to support new features and to change its settings and configurations, or to be uninstalled when it is no longer providing valuable intelligence to the organization.

Agent Upgrade

When agent upgrades are released and available to install. These new agents are now ready for installation on new targets' devices or as existing upgrades of installed agents on targets' devices. These updates provide new functionalities, bug fixing, supporting new services or improving the agents' overall behavior. Such upgrades are crucial to keep the agent functional and operational given the endless advances in the world of communications, particularly the Smartphone area.

There are two types of agent upgrades:

- **Optional upgrade:** Not mandatory by the system. The user decides when, if at all, to upgrade the agent.
- **Mandatory upgrade:** Mandatory by the system. The supervisor must upgrade the agent, otherwise no new information will be monitored from the device.

Upgrade sometimes requires a new agent installation and, sometimes, just a small existing agent upgrade. In both cases the user is the only one to decide when to the upgrade and, therefore, should plan this accordingly.

Once the upgrade command was sent by the user, the process should take only a few minutes. The process could take longer if the device is turned off or has data connection. In any event, the upgrade will be accomplished once a decent data connection becomes available.

Agent Settings

Sometimes, installation of new agent and agent is required to set settings for the first time during its installation. From this point, these settings serve the agent, but they can always be changed if required. The settings include the IP address for transmitting the collected data, the way commands are sent to the agent, the time until the agent is automatically uninstalled (see self-destruction mechanism for more details) and more.

Agent Uninstall

When the intelligence operation is over or in the event target is no longer of interest to the organization, the software-based component ("agent") on the target's device can be removed and uninstalled. Uninstall is quick, requires a single user request and has zero to minimal effect on the target's device. The user subjects [?] a request for agent uninstall which is sent to the device.

Once agent is uninstalled from a certain device, it leaves no trace whatsoever or indication that it ever existed 4.

As long as the agent is operational on the device and a connection exists between it and the servers, it can be easily and remotely uninstalled.

.

Uninstall can always be done remotely, regardless of the method used for installation.

Physical uninstall is also an option, if necessary.

Uninstalling an agent does not mean losing the entire collected data – all data collected during the time the agent was installed on the device will be kept in the servers for future analysis.

Self-Destruct Mechanism

The Pegasus system contains a self-destruct mechanism for the installed agents. In general, it is understood it is more important than the origin, and the targets will not be exposed to anything suspicious than keeping the agent alive and working [?]. The mechanisms [*sic*] are activated under the following scenarios:

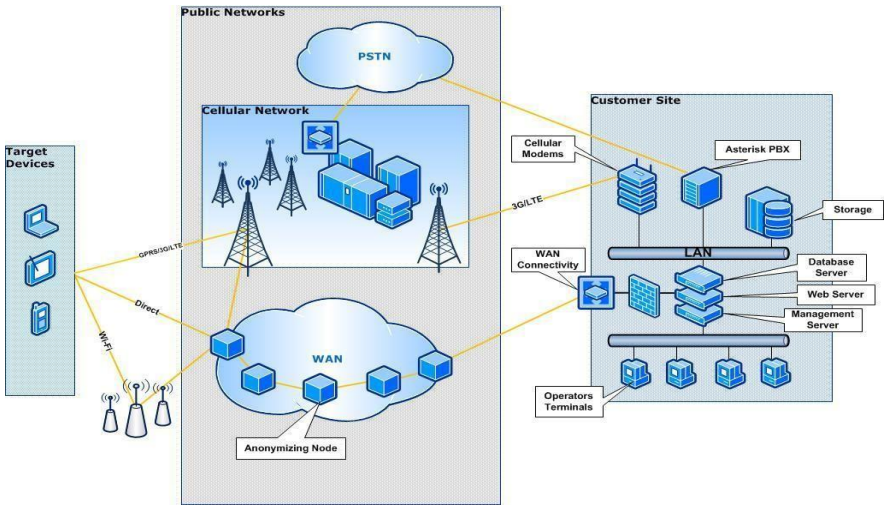
- **Risk of exposure**: In cases where there is a high likelihood of exposing the agent, the self-destruct mechanism is automatically activated and the agent is uninstalled. Agent can be installed once again at a later time.

- **Agent not responding**: In cases where the agent is not responding and did not communicate with the servers for a long time, the agent will automatically uninstall. To be exposed to it or misused [?].

Solution Architecture

The Pegasus system's major architectural components are shown in Figure 10.

Figure 10: Solution Architecture



Customer's Site

NSO is responsible for deploying and configuring the Pegasus hardware and software at the customer's premises, making sure the system is working and operating properly. The main components installed at the customer site are listed below:

Web Server

Located at the customer's premises, the servers are responsible for the following:

- Agent installation and maintenance
- Monitoring agent: Remotely control, configure and upgrade installed agents
- Data transmission: Receive the collected data transmitted from the installed agents
- Operators' terminals

Communications Module

The communications module allows interconnectivity and Internet connection to the servers.

Cellular Communication Module

The cellular communication module enables remote installation of the Pegasus agent on the target's device by using cellular modems or SMS gateways.

Permission Module

The Pegasus permission management module defines and controls the features and the available content allowed for each user based on their role, rank and hierarchy.

Data Storage

The collected data extracted and monitored by the agents are stored on an external storage device. The data are properly backed-up, with full resiliency and redundancy to prevent failures and downtime.

Servers Security

All servers reside within the customer's trusted network, behind the security measures it may implement, as well as security measures specifically provided by us for the system.

Hardware

The system's standard hardware is deployed on several servers connected together [in a] couple of racks. The equipment is responsible for advanced load balancing, content compression, connection management, encryption, advanced routing, and highly configurable monitoring server of monitoring status [?].

Operator Consoles

The operator's end-point terminals (PC) are the main tool for the operators to activate the Pegasus system, to initiate installations and commands and to view the collected data.

Pegasus Application

The Pegasus application is the user interface installed on the operator terminal. It provides the operators with the range of tools to view, sort, filter, manage and alert in order to analyze the large amount of collected data from the targets' agents.

Public Networks

Apart from hardware and software installation at the customer's premises, the Pegasus system does not require any physical interface with the local mobile network operators. However, since data and agent installations are transferred over public networks, wemakes [*sic*] it is transferred in the most efficient and safe way, all the way back to the customer's servers.

Anonymyzing Networks

Pegasus anonymizing transmission network (Network) is built from anonymizing connectivity nodes which are spread in various locations around the world, allowing agent connections to be directed through different paths prior to reaching the Pegasus servers. The anonymized nodes serve only one customer and can be set up by the customer, if required.

See more information in the Pegasus Anonymizing Transmission Network section.

Target Devices

The above-mentioned architecture allows operators to issue new installations, extract, monitor and actively collect data from targets' devices.

Note: Pegasus is an intelligence mission-critical system; therefore, it is fully redundant to avoid malfunctions and failures. The system handles large amounts of data and traffic 24 hours a day and is scalable to support customer growth and future requirements.

Hardware Solution

The hardware specifications for operating the Pegasus system depend on the number of concurrent installed agents, the number of work stations, the amount of stored data and how long the data should be stored.

All the necessary hardware is supplied with the system upon deployment and may require local customization, which has to be managed by the customer based on directions. If required, hardware can be purchased by the customer based on the specifications provided by us.

Terminals' Operators

The terminals' operators are standard desktop PCs, with the following specifications:

- Processor: Core i5
- Memory: 3GB RAM
- Hard Drive: 320GB
- Operating System: Windows 7

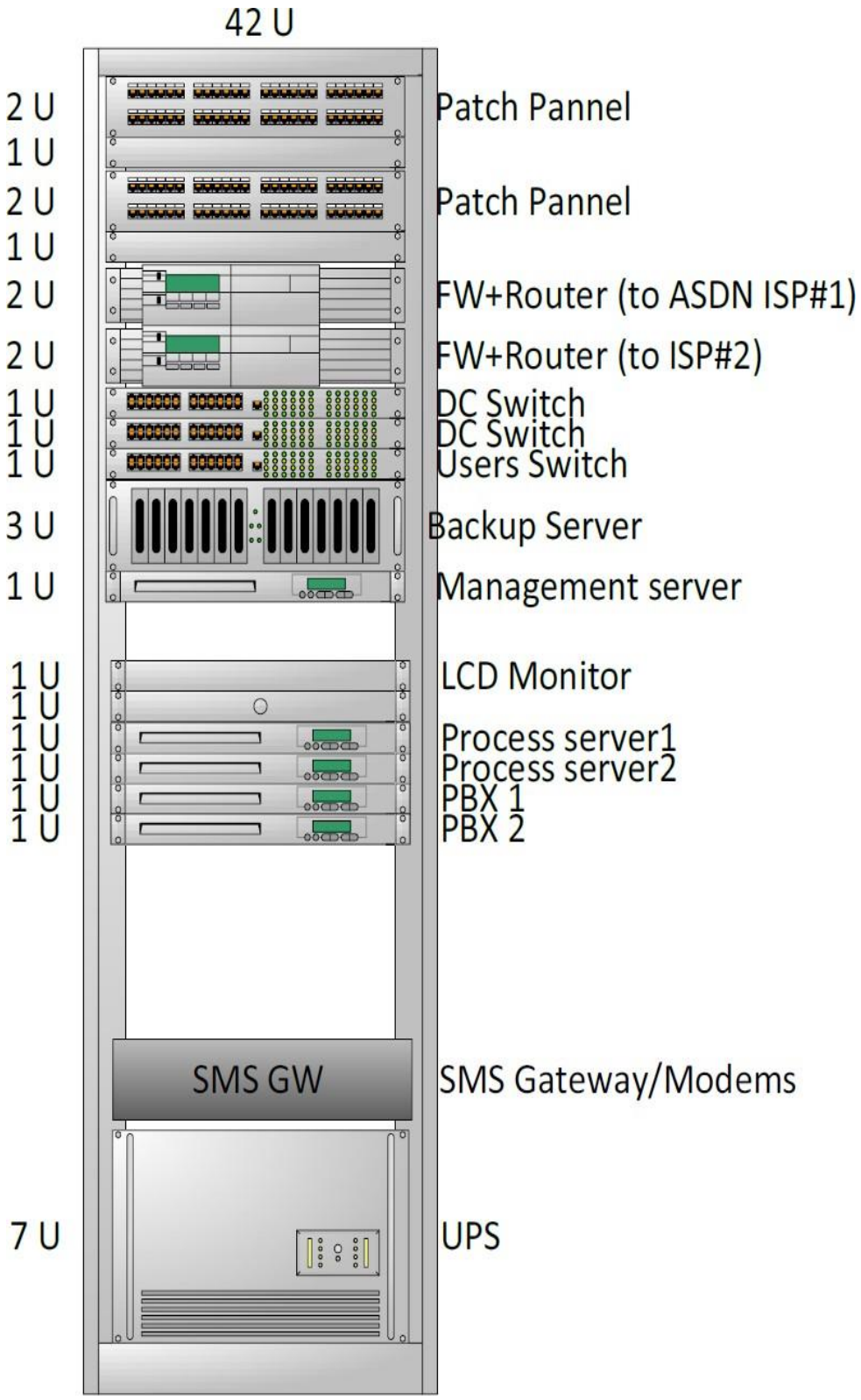
System's Hardware

To fully support the system's infrastructure, the following hardware is required:

- Two 42U cabinet units
- Networking hardware
- 10TB of storage
- 5 standard servers
- UPS
- Cellular modems and SIM cards

The system's hardware scheme is shown in Figure 11.

Figure 11: Pegasus Hardware



[LOGO] PGR – PROCURADURÍA GENERAL DE LA REPÚBLICA
OFFICE OF THE ATTORNEY GENERAL OF THE REPUBLIC

Classification Date	Mexico, F.D., October 16, 2014
Administrative Unit	Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia (National Planning, Analysis and Information Crime Fighting Center)
Classification	Confidential
Privileged or Confidential Portions or Sections	In full
Legal Basis	13 pars I, IV and V, and 14 par. 1, Federal Transparency and Access to Public Government Information Act. Rule Eighteenth, pars. II and V, subpars. c) and d) and Twenty-Fourth, par. II, General Guidelines for Classifying and Declassifying Information from the Federal Public Administration's offices and agencies.
Specific Law	Section 40, par. XXI of the Act establishing the Basis of the National Public Security System
Confidentiality Period	Up to 12 years * (*sic*)
Signature of Administrative Unit Incumbent	